جنگ نرم ۱

ویژه جنگ رایانه‌ای

موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران

جنگ نرم ۱

ویژه جنگ رایانه‌ای

سلسله انتشارات مؤسسهٔ فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران

ضیایی‌پرور، حمید
جنگ نرم ۱: ویژه جنگ رایانه‌ای/ گردآوری و تدوین حمید ضیایی‌پرور؛ نظارت و اجرا مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، معاونت تولید؛ ویراستار سارا جوادی. - تهران: مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، ۱۳۸۳.
۴۲۳ ص.
ISBN 978-964-526-131-1: ۸۵۰۰۰ ریال
فهرست‌نویسی براساس اطلاعات فیپا.
واژه‌نامه.
۱. جرائم کامپیوتری. ۲. کامپیوترها — صنعت و تجارت. ۳. رقابت‌های بین‌المللی. ۴. هکرها. الف. مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران. ب. عنوان.
۳۶۴/۱۶۸ HV۶۷۷۳/۹ج۹ض
کتابخانه ملی ایران ۸۳_۲۱۹۴۷م

انتشارات مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران
تهران: صندوق پستی ۳۸۴۹ ـ ۱۵۸۷۵، تلفن: ۸۸۵۰۰۲۵۰، نمابر: ۸۸۷۵۶۲۰۷
نشانی اینترنت:www.tisri.org پست الکترونیک: info@tisri.org

جنگ نرم (۱) (ویژه جنگ رایانه‌ای)

نظارت و اجرا: مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران ـ معاونت پژوهشی
گردآوری و تدوین: حمید ضیایی‌پرور
ویراستار: سارا جوادی
صفحه‌آرا: علی اکبر حسینیه فراهانی
حروفچین: منصوره سعادت، پروانه اکبری
نمونه‌خوان: سمانه ضرابی‌نژاد
طراح جلد: مریم جعفری نائینی
چاپ نخست: شهریور ماه ۱۳۸۳
چاپ دوم: فروردین ماه ۱۳۸۶
چاپ سوم: اسفند ماه ۱۳۸۷
چاپ چهارم: مهرماه ۱۳۸۸
چاپ پنجم: آذرماه ۱۳۸۸
چاپ ششم: دی‌ماه ۱۳۸۹
چاپ و صحافی: باقری
شمارگان: ۱۰۰۰ نسخه
قیمت: ۸۵۰۰ تومان
شابک: ۹۷۸_۹۶۴_۵۲۶_۱۳۱_۱
کدبازیابی در کتابخانه دیجیتالی دید: BB00020040308001915

فهرست

فصل سوم

فصل چهارم

بخش دوم: تکنیک‌های جنگ رایانه‌ای

فصل اول

فصل دوم

بخش سوم: جنگ رایانه‌ای در ایران

ضمائم

مقدمه

پروژه جنگ نرم، یکی از مهم‌ترین فعالیت‌های پژوهشی مؤسسه تهران است که زمان آغاز فاز تحقیقی آن به بهار ۱۳۸۲ بازمی‌گردد. هدف این پروژه، شناخت مبانی و اصول و همچنین آشنایی با تکنیک‌ها و فنون جنگ نرم است. به همین دلیل، مؤسسه تهران تصمیم بر آن گرفت تا نتایج این پژوهش را در قالب کتاب‌هایی با عنوان کلی «جنگ نرم» و زیرعنوان‌های مربوطه چاپ نماید. در این راستا، نخستین جلد از مجموعه فوق، ویژه جنگ رایانه‌ای نام گرفته و به چاپ رسیده است. این کتاب به بررسی جنبه‌های مختلف تکنولوژی رایانه‌ای و نرم‌افزاری و کاربرد آن در جنگ پرداخته و زمینهٔ مناسبی را برای تحقیقات بیشتر بر روی هر یک از موضوعات فراهم می‌آورد. درمجموع، جنگ رایانه‌ای اشاره به وضعیتی دارد که در آن عملیات نظامی بر اساس اطلاعات رایانه‌ای، کنترل شده و به منظور جلوگیری از عملیات دشمن و همچنین ایجاد اختلال در ارتباطات و جلوگیری از دسترسی وی به اطلاعات، تلاش می‌شود.

مجموعه حاضر از سه بخش تحت عناوین «تعاریف و انواع جنگ رایانه‌ای»، «تکنیک‌های جنگ رایانه‌ای» و «جنگ رایانه‌ای در ایران» تشکیل شده که در بخش اول به تعاریف هک کردن، نفوذ به کامپیوترها و جرایم اینترنتی، در بخش دوم به استراق سمع، ردیابی، کلاهبرداری مخابراتی، حسگرها، ماهواره‌ها، پارازیت و بررسی و نرم‌افزارهای جاسوسی و در بخش سوم نیز به مسائل مختلف دررابطه با اینترنت در ایران می‌پردازد.

لازم به ذکر است دومین جلد از مجموعه کتاب‌های «جنگ نرم» با تمرکز بر «جنگ رسانه‌ای» به زودی چاپ و در اختیار علاقمندان قرار خواهد گرفت.

مؤسسهٔ فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران

بخش اول

تعاریف و انواع جنگ رایانه‌ای

فصل اول

۱ـ۱ـ جنگ رایانه‌ای[1]

جنگ رایانه‌ای اشاره به وضعیتی دارد که در آن عملیات نظامی براساس اطلاعات رایانه‌ای[2] کنترل شوند و یا به‌منظور جلوگیری از عملیات دشمن برای ایجاد اختلال در ارتباطات[3] و جلوگیری از دسترسی وی به اطلاعات تلاش شود. معنای دیگر جنگ رایانه‌ای، تلاش برای کسب اطلاعات هرچه بیشتر درباره دشمن و جلوگیری از کسب اطلاعات توسط وی درباره شما است یا به تعبیری، تلاش برای تغییر توازن اطلاعات[4] و دانش به نفع شما، به‌خصوص در وضعیتی که توازن نیروهای نظامی به نفع شما نیست و در نهایت جنگ رایانه‌ای به معنای استفاده از اطلاعات برای به حداقل رساندن سرمایه، جنگ‌افزار[5] و نیروی انسانی[6] مورد نیاز برای کسب پیروزی در جنگ است. این نوع جنگ، نیازمند تکنولوژی‌های مختلفی است. به‌خصوص برای صدور فرمان‌ها و کنترل میدان جنگ، جمع‌آوری هوشمندانه اطلاعات و پردازش و صدور آنها، ارتباطات تاکتیکی[7]، موقعیت‌یابی، تشخیص دوست از دشمن و در نهایت برای استفاده از سلاح‌های هوشمند[8] که قادرند به‌صورت اتوماتیک براساس اطلاعات دریافتی از ماهواره بر علیه دشمن بجنگند.

---

1. Cyber war
2. Computer Information
3. Derangement in Communication
4. Information Balance
5. Weapons
6. Staffing
7. Tactical Communications
8. Intelligence weapons

جنگ رایانه‌ای، اصول جنگی و نهادهای کنترلی جدیدی می‌آفرینند. لازمه ایجاد و حرکت به سمت شبکه‌های جنگی، تمرکززدایی در روند فرماندهی جنگ است که باعث خواهد شد تا نیروهای درگیر در جنگ بتوانند با اطلاعات دقیق از وضعیت خود، در هر لحظه بهترین تصمیم‌گیری را انجام داده و به آن عمل نمایند، اما این فقط یک روی سکه است. استفاده از تکنولوژی اطلاعات[1] در عین حال باعث خواهد شد تا مقر اصلی فرماندهی، دیدی وسیع نسبت به تمامی میادین جنگ و وضعیت دقیق نیروهای طرفین داشته باشد و این تمرکززدایی در عین دید از بالای مرکز فرماندهی، راز قدرتمندی ارتش‌هایی است که از تکنولوژی اطلاعات استفاده می‌نمایند. همان‌گونه که گفته شد، جنگ‌های رایانه‌ای، اصول جنگی جدیدی را جایگزین اصول قدیمی نموده‌اند. نوع نیروهایی که در این‌گونه جنگ‌ها شرکت می‌کنند، نحوه استفاده از آنها و حتی نحوه یورش به سوی دشمن، (استراتژی جنگی) نیز با گذشته تفاوت‌های بسیار عمیقی پیدا کرده است. امروزه تصمیم‌گیری در مورد تعداد، نوع و مکان استفاده از حسگرها[2]، کامپیوترها[3]، شبکه‌ها[4] و بانک‌های اطلاعاتی[5] که در جنگ مورد استفاده قرار می‌گیرند، همان اهمیتی را پیدا کرده که در جنگ جهانی دوم در مورد زمان و نحوه استفاده از بمب‌افکن‌ها در پشت خط مقدم دشمن، مطرح می‌شد.

به‌عنوان یک نوآوری در استراتژی‌های جنگی، جنگ رایانه‌ای قرن ۲۱ را می‌توان با «بلیتز کریگ» قرن ۲۰ مقایسه کرد. جنگ رایانه‌ای، بلیتز کریگ عصر اطلاعات است. بلیتز کریگ یا «جنگ رعدآسا» نوعی از استراتژی جنگی است که در ابتدا توسط آلمانی‌ها در اسپانیا در سال ۱۹۳۸ و سپس علیه لهستان در سال ۱۹۳۹ به‌کار گرفته شد. در این نوع جنگ، با حمله بسیار سریع و همه‌جانبه و با حمایت توپخانه و تانک تلاش می‌شود تا دشمن غافلگیر شده و پیش از آنکه بتواند عکس‌العمل نشان دهد، از پای درآید.

---

1. Information Technology
2. Sensors
3. Personal Computers
4. Networks
5. Information Banks

در جنگ رایانه‌ای، برتری در کسب[1]، کنترل[2]، پردازش[3] و انتقال اطلاعات[4] و تلاش برای جای‌گیری صحیح، کشف نقشه‌های دشمن و حمله به ضعیف‌ترین و حساس‌ترین نقطه‌های خطوط دفاعی در مناسب‌ترین لحظات قبل از اینکه دشمن حتی متوجه نقاط ضعف خود شود، از اهمیت شایان توجهی برخوردار است. میدان نبرد پست مدرن[5] با استفاده از تکنولوژی اطلاعات در زمینه‌های استراتژیکی و تاکتیکی نسبت به گذشتهٔ خود تغییر خواهد کرد. در طول تاریخ و در اکثر دیدگاه‌های سنتی نسبت به ارتش، ارتشیان دارای سلسله مراتب کاملاً دقیقی بوده و نیروها به اجرای دقیق و بی‌چون و چرای دستورات مافوق خود افتخار می‌کردند. در این ارتش‌ها، تمامی دستورات دقیقاً از بالا دیکته می‌شد و سربازان پایین‌تر بدون چون و چرا آنها را اجرا می‌کردند. اما امروزه، انقلاب اطلاعاتی[6] باعث ایجاد تغییراتی در این وضعیت شده و سلسله مراتب ارتشی در معنای قدیمی خود منسوخ شده و برای فرمانبرداری نظامی، مرزهای جدیدی در حال تعریف است.

برای مثال، مغول‌ها در قرن ۱۳ براساس جنگ اطلاعاتی امروزین، خود را سازمان داده و بیشتر شبیه به یک شبکه بودند تا سلسله مراتبی منظم. به‌عنوان نمونه‌ای امروزی‌تر، می‌توان از ویت‌کنگ‌هایی که در جنگ آمریکا و ویتنام می‌جنگیدند، نام برد. نیروی نظامی نسبتاً کوچکی که در برابر یکی از بزرگ‌ترین نیروهای نظامی قرن حاضر به خوبی ایستادگی کرد. ویت‌کنگ‌ها نیز بیشتر به نظامی شبکه‌ای شبیه بودند تا سیستمی مبتنی بر سلسله مراتبی رسمی. در هر دو مثال بالا نیروهایی که در برابر مغول‌ها و ویت‌کنگ‌ها می‌جنگیدند، مؤسسات بزرگ و نهادینه شده‌ای بودند که برای جنگ‌های فرسایشی و منظم ترتیب داده شده و به‌طور دقیق از سلسله مراتب نظامی تبعیت می‌کردند و همچنین تمامی دستورات از فرماندهان رده بالا صادر می‌شد.

---

1. Getting
2. Control
3. Process
4. Transfer of Information
5. Post Modern Warfare
6. Information Revolution

در سیستم‌های سنتی و مبتنی بر سلسله مراتب هر یک از رزمندگان، دستورات مربوط به نحوه عملشان را مستقیماً از مقام بالاتر خود می‌گیرند و مقامات بالاتر نیز به نوبه خود از مقامات ارشدتر کسب تکلیف می‌کنند، اما در سیستم شبکه‌ای اعضا با استفاده از اطلاعاتی که در اختیار دارند و براساس هدف نهایی که رهبر اصلی تعیین می‌کند، عمل می‌نمایند. این سیستم به رزمندگان، استقلال عمل داده و در نتیجه آنها را بسیار تحرک‌پذیر و هوشمند می‌سازد. از طرف دیگر، در این سیستم‌ها، نقش دستوردهی و تعیین اهداف جزئی، از دوش فرماندهان عالی برداشته شده، در نتیجه افراد با استفاده از اطلاعات کاملاً دقیق، وضعیت نیروها، پردازش اطلاعات و آمار و تحلیل کامپیوتری آنها خواهند توانست، نسبت به اتخاذ بهترین تصمیم و اعلام آن به‌صورت اهداف جنگی به نیروهای مستقل، کل شبکه را در رسیدن به پیروزی نهایی یاری رسانند. در این وضعیت، میدان نبرد، بیشتر شبیه به یک مسابقه شطرنج در سطح جهانی است تا یک مسابقه بوکس حرفه‌ای. زمانی‌که مغول‌ها به جهان‌گشایی پرداختند، تعداد جنگجویان آنها بسیار کمتر از تعداد جنگجویان کشورهایی بود که مورد هجوم قرار می‌گرفتند، اما مغول‌ها در جنگ پیروز شدند و برای بیش از یک قرن، بزرگ‌ترین امپراتوری طول تاریخ را ایجاد کردند. کلید پیروزی آنها احاطه دقیق و کامل بر اطلاعات میدان جنگ بود. مغولان دقیقاً در زمان و مکانی که برای شکست دادن دشمن مناسب بود، حمله می‌کردند و پیکان سواران آنان نیز روزانه دستورات فرماندهان را به جنگجویان منتقل می‌نمودند که در برخی مواقع بین این دو ارتش بیش از صدها کیلومتر فاصله بود. خان بزرگ حتی در مواقعی که هزاران کیلومتر با میدان‌های نبرد فاصله داشت نیز به‌طور دقیقی از اخبار جنگ مطلع گردیده و دستورات لازم را صادر می‌کرد.[1]

۲ـ۱ـ جنگ بر روی شبکه NCF

پیشرفت تکنولوژی اطلاعاتی (IT) و شبکه‌های رایانه‌ای باعث شد تا صنایع نظامی نیز از این مسئله تأثیر پذیرفته و به سمت رایانه‌ای‌تر شدن پیش روند. امروزه حتی صحبت از چیزی به

نام «جنگ از راه دور»[1] به میان می‌آید، جنگی که در آن فرماندهان و افسران از نقطه‌ای بسیار دور مستقیماً عملیات نظامی در یک منطقه جنگی را به‌دست گرفته و آنرا هدایت می‌کنند. «براساس گزارشی که رادیو آمریکا مخابره کرده، وزارت دفاع آمریکا، پنتاگون قصد دارد سیستم‌های تسلیحاتی و نظامیان را در شبکه‌ای ادغام کند که اصطلاحاً «NCF» یا جنگ مبتنی بر شبکه نامیده می‌شود. از نوامبر سال ۲۰۰۲، خلبانان نیروی هوایی آمریکا به آخرین نسخه از یک بازی ویدئویی دست یافتند. آنها می‌توانند از طریق هر کامپیوتر معمولی PC[2] که دارای یک کاوشگر اینترنتی[3] و یک نرم‌افزار ویژه نظامی باشد به شبکه کامپیوتری نیروی هوایی آمریکا متصل شوند. هنگامی که به شبکه وصل شدند، می‌توانند هواپیماهای شناسایی (بدون سرنشین) را به طرف هدف، راهنمایی کرده و یا تقاضای حمله هوایی کنند. آنها حتی از طریق یک کامپیوتر دستی یا لپ‌تاپ[4] متصل به اینترنت می‌توانند مسیر پرواز را طراحی کنند» استفاده نظامی از شبکه اینترنت مسئله عجیبی قلمداد نمی‌شود. نباید از یاد برد که ابداع و اختراع اینترنت، توسط نظامیان و به‌خصوص وزارت دفاع آمریکا صورت گرفته است. در اواسط دهه ۹۰م. راه‌حل وزارت دفاع آمریکا برای متصل کردن سیستم‌های نظامی مختلف به زیر یک چتر، به‌گونه‌ای که حتی اگر یک بخش دچار صدمه و اخلال شود، بخش‌های دیگر به کار خود ادامه دهند، پروژه‌ای به نام آرپانت[5] بود که پدر اینترنت فعلی به‌شمار می‌رود. پروتکل ارتباطی TCP-IP شاهرگ اصلی اینترنت به‌شمار می‌رود که به کامپیوترهای مختلف با سیستم‌های عامل مختلف این اجازه و امکان را می‌دهد تا با یکدیگر گفت‌وگو و تبادل اطلاعات کنند. در حال حاضر هم بخش عمده‌ای از ارتباطات رایانه‌ای پنتاگون بر روی همین اینترنت عمومی که شکل توسعه‌یافته و عمومی شده آرپانت است، صورت می‌گیرد.

یکی از مشکلات اصلی بهره‌برداری نظامی از اینترنت، سرعت آن است. حجم اطلاعات

1. Faraway Warfare
2. Personal Computer
3. Browser
4. Laptop
5. Arpanet

مورد نیاز در یک عملیات نظامی به قدری بالا و سنگین است که می‌تواند کمر هر شبکه‌ای را بشکند. وزارت دفاع آمریکا برای غلبه بر این مشکل در نظر دارد تا سال ۲۰۰۴ خطوط انتقال داده‌هایش را در ۹۰ منطقه استراتژیک جهان به یک گیگابیت در ثانیه برساند که حدود ۸ برابر بیشتر از یک خط اختصاص IT است. اما همچنان باز هم مشکل موسوم به «یک کیلومتر آخر» یعنی نقطه خروجی داده‌ها که سنگین‌ترین ترافیک الکترونیک را پیدا می‌کند، باقی است. ارتش آمریکا بر روی چند راه‌حل برای این قسمت از اشغال خطوط کار می‌کند که عبارتند از:

۱. استفاده از لیزرهای قدرتمند برای انتقال داده‌ها از ماهواره به زمین و از روی کوهی به کوه دیگر.

۲. تکنولوژیی است که هر وسیله نقلیه نظامی را تبدیل به یک گره[1] در شبکه بی‌سیم[2] می‌کند. چنین گره‌ها یا نقاط رله‌کننده‌ای که از یک زره‌پوش تا هلی‌کوپتر را دربر می‌گیرد، می‌توانند در اطراف یک میدان جنگ، یک شبکه در هم تنیده مخابراتی را به‌وجود آورند.

اما هنوز تا رسیدن به این ایده‌ها، راه درازی در پیش است. مشکل اصلی، خراب شدن گاه و بی‌گاه کامپیوترها است. اگر یک کامپیوتر درست در زمانی خاص از کار بیفتد، تکلیف عملیات نظامی چه خواهد بود؟ استفاده کارآمد از یک پرسنل معین، باید بتواند دقیقاً در لحظه درست، اطلاعات صحیح را در اختیار داشته باشد. راه‌حل این قضیه در پروتکل ارتباطی جدیدی به نام XML است که به نحوی هر تکه از داده‌ها را علامت می‌زند و نرم‌افزار در مسیر حرکت خود می‌داند هر قسمت از داده به کدام سنگر و نقطه باید توزیع شود.

استفاده از جنگ مبتنی بر شبکه، مشکلاتی نیز به همراه دارد. طرفداران NCF به‌عنوان بهترین دلیل برای روی آوردن به جنگ شبکه‌ای، از جنگ افغانستان (حمله آمریکا به افغانستان پس از ۱۱ سپتامبر) نمونه می‌آورند. در آن جنگ، سه نیروی زمینی، دریایی و هوایی آمریکا در یک هماهنگی بی‌سابقه با هم کار کردند اما به‌رغم این موفقیت، بسیاری از فرماندهان، وقتی با

1. Node

2. Wireless Network

محدودیت‌های جنگ شبکه‌ای برخورد کردند، سرخورده شدند. همه این داستان را شنیده‌اند که چطور نیروهای ویژه ارتش آمریکا در افغانستان، از روی زمین با یک لیزر مخصوص، هدف‌ها را نشانه می‌گرفتند و هواپیماهای جنگنده را دقیقاً به هدف رهنمون می‌کردند. اما چیزی که در رسانه‌ها بیان نشد، این بود که فرماندهان باید برای وقت تماس با ماهواره Uplink صف می‌کشیدند و بر سر اینکه چه کسی باید از هواپیمای شناسایی بدون سرنشین UAV استفاده کند با یکدیگر بحث می‌کردند. بسیاری از افسران نیز از ناکافی بودن ظرفیت انتقال داده‌ها در کابل‌ها یا امواج موجود Bandwith شکایت داشتند. جنگ مبتنی بر شبکه، یک نقطه ضعف اساسی دیگر نیز دارد. فرماندهی که از راه دور به کنترل عملیات می‌پردازد اغلب، بخش اصلی و تعیین‌کننده اطلاعات منطقه‌ای و محلی را نمی‌داند![۲]

۳ـ۱ـ مانور مجازی[۱]

براساس قراردادی که بین آمریکا و قطر امضا شد، مقامات قطر با تکمیل و بازسازی یک پایگاه هوایی متعلق به آمریکا در این کشور موافقت کردند. این پایگاه دارای بلندترین باند پرواز در خاورمیانه به طول ۵ کیلومتر است. تجهیزات این پایگاه با آخرین فناوری‌های الکترونیکی و صنعتی تکمیل خواهد شد و در آن از سیستم‌های رایانه‌ای بسیار قوی استفاده می‌شود. براساس گزارش رادیو BBC، رامسفلد، وزیر دفاع آمریکا که این قرارداد را در قطر امضا کرد با ژنرال تومی فرانکس، رئیس ستاد فرماندهی عملیات در منطقه از تجهیزات جدید مخابراتی، اینترنتی و الکترونیکی میان نیروهای دریایی، هوایی و زمینی آمریکا و نیروهای ویژه و تفنگداران دریایی در منطقه بازدید کرد. وی از پایگاه ویژه نیروهای آمریکا در قطر با فرماندهان عملیاتی آمریکا در بحرین و عربستان گفت‌وگوی ویدئویی داشت و طرح‌های نظامی برای حمله به عراق را که به‌صورت بازی‌های ویدئویی و اینترنتی طراحی شده بود، مورد بازدید قرار داد.

---

1. Cyber Manoeuvre

مدتی بعد، علاوه بر مانور حقیقی که در آب‌های خلیج‌فارس صورت گرفت چندین مانور مجازی که در آن به جای سربازان، کارشناسان آمریکایی و بریتانیایی از نرم‌افزارهای کامپیوتری[1] و شبیه‌سازی‌ها[2] استفاده کردند، انجام شد. به گزارش رادیو آمریکا، آزمایش تکنولوژی‌های مدرن ارتباطات[3] و مخابرات و کنترل و فرماندهی بخشی از آزمایش‌هایی بوده که در این قرارگاه صورت گرفته است.(۳)

۴ـ۱ـ استراتژی رخنه رایانه‌ای

دولت آمریکا ماه‌ها پیش از شروع جنگ علیه عراق، در راستای جنگ اطلاعاتی[4] و عملیات روانی[5] خود علیه این کشور، استراتژی معینی را تحت عنوان «استراتژی رخنه و ایجاد اختلال در سیستم‌های رایانه‌ای دشمن» تصویب کرده بود. براساس این استراتژی، ماه‌ها و هفته‌ها پیش از شروع جنگ، باید سیستم‌های ارتباطی رایانه‌ای عراق شناسایی می‌شد و عملیات لازم برای نفوذ و ایجاد اختلال در عملکرد آنها صورت می‌گرفت. روزنامه واشنگتن پست در گزارشی که دو هفته پیش از شروع جنگ در عراق منتشر کرد، فاش نمود که آمریکا سرگرم بررسی و طرح‌ریزی برای دست زدن به حملات اینترنتی علیه کشورهایی مانند عراق است. این حملات قرار بود پیش از شروع عملیات نظامی یا همزمان با آن صورت گیرد. سایت اینترنتی BBC دو روز پس از انتشار گزارش واشنگتن پست، چنین نوشت: «در هرگونه نبرد اینترنتی علیه عراق باید نقشی را که رایانه‌ها در اداره امور این کشور ایفا می‌کنند، مدنظر قرار داد». دی کی ماتای، مدیر شرکت اینترنتی "MIZJ" می‌گوید: «عراق دارای تأسیسات ارتباطی نسبتاً پیشرفته‌ای است و هرگونه حمله رایانه‌ای ممکن است خدمات اضطراری این کشور را فلج کرده و غیرنظامیان و نظامیان را از ارتباط با یکدیگر محروم سازد».

---

1. Software
2. Similar
3. Modern Communication Technology
4. Information Warfare
5. Psychological Operations

از کار انداختن شبکه‌های ارتباطی، شیوه تازه‌ای در جنگ نیست و نبرد اطلاعاتی همواره بخشی از استراتژی نظامی کشورهای مختلف بوده است.

در همان زمان «مایک نایتس»، کارشناس نبردهای اینترنتی در نشریه تخصصی نظامی «جینز دیفنس»[1] می‌گوید: «بعید است که آمریکا سیستم‌های رایانه‌ای عراق را به کمک شیوه‌های پیشرفته (نفوذ و اخلال اینترنتی)[2] هدف قرار دهد. به گفته وی، رایانه‌های عراقی که اطلاعات حساسی[3] در آنها ذخیره شده به شبکه متصل نیستند و بنابراین در مقابل حمله اینترنتی نیز آسیب‌پذیر نخواهند بود. او ادعا کرد که ارتش آمریکا هرگز حملات رایانه‌ای را بخش مهمی از جنگ اطلاعاتی علیه عراق قلمداد نکرده است. چند دهه طول خواهد کشید تا این شیوه به بخش مهمی از استراتژی نظامی تبدیل شود، مشاهده تأثیر حملات رایانه‌ای[4] همیشه آسان نیست و درک توپوگرافی[5] شبکه‌های رایانه‌ای به‌ویژه شبکه‌های ابتدایی، مانند آنچه عراق دارد، دشوار است، اما به گفته وی این مسئله، آمریکا را از به راه انداختن جنگ روانی از طریق پست الکترونیکی[6] بازنداشته است.

پیش از شروع جنگ، برای ژنرال‌های عراقی نامه‌هایی الکترونیکی که در آن آمده است که ما تو را شخصاً می‌شناسیم، ارسال گشت و از آنها خواسته شد تا با ارسال علائم نوری در طول جنگ، محل اختفای سلاح‌های کشتار جمعی را مشخص کنند. عراق یکی از آخرین کشورهای خاورمیانه می‌باشد که به شبکه اینترنت متصل شده است، اما تنها ۱۲ هزار نفر از جمعیت ۲۳/۵ میلیونی آن به شبکه جهانی اینترنت دسترسی دارند، البته میزان دسترسی مردم شمال عراق به اینترنت که فارغ از حکومت صدام زندگی می‌کردند، بسیار بیشتر بوده است.

در مقابل، آمریکا به‌شدت به سیستم‌های رایانه‌ای[7] وابسته است. در پی حملات تروریستی ۱۱ سپتامبر علیه این کشور، دولت آمریکا تدابیر امنیتی در اینترنت[8] را تشدید کرد. جورج

1. Jane's Defense
2. Internet Hacking
3. Top-Secret Information
4. Cyber Attacks
5. Topography
6. E-mail
7. Computer System
8. Security Policies in Internet

بوش، رئیس‌جمهور آمریکا دستور داد ۱/۵ میلیارد دلار بر بودجه تدابیر امنیتی شبکه‌های رایانه‌ای و اینترنتی و همچنین آموزش متخصصانی که با حملات اینترنتی احتمالی تروریستی مقابله می‌کنند، افزوده شود. وزارت دفاع آمریکا، پنتاگون از یک سال پیش، حدود هزار هکر حرفه‌ای را به استخدام خود درآورده تا از آنها برای نفوذ به شبکه‌های رایانه‌ای کشورهای مورد هدف یا گروه‌های مورد نظر آمریکا استفاده کند.

به گفته متخصصان رایانه و شبکه، اگرچه آمریکایی‌ها از لحاظ به راه انداختن نبرد اطلاعاتی مبتنی بر اینترنت در جهان کم‌نظیرند، اما از سوی دیگر آمریکا بیش از سایر کشورها در مقابل حملات اینترنتی متقابل آسیب‌پذیر است.

اتکای شبکه‌های برق‌رسانی، بانکداری، تجارت و اقتصاد، خدمات عمومی، روابط دستگاه‌ها و وزارتخانه‌ها، فرودگاه‌ها، تأسیسات عمومی، شرکت‌ها و مؤسسات خصوصی و دولتی به اینترنت، آسیب‌پذیری ساختار آمریکا را نسبت به یک حمله گسترده اینترنتی بیشتر کرده است. تنها یک ویروس اینترنتی به نام Slammer در مدت زمان کوتاهی توانست ۱۳ هزار دستگاه عابر بانک در آمریکا را از کار بیندازد و در نتیجه خدمات اضطراری در شهر سیاتل را مختل کند.(۴)

۵ـ۱ـ تروریسم رایانه‌ای[1]

«تروریسم رایانه‌ای» واژه جدیدی می‌باشد که به ادبیات سیاسی جهان وارد شده است. این نوع عملیات تروریستی به هرگونه اقدامات خرابکارانه‌ای اطلاق می‌شود که نفوذگران[2] و اخلالگران رایانه‌ای علیه شبکه‌های رایانه‌ای و اینترنتی یک کشور انجام می‌دهند. اکنون شبکه اینترنت، بستر و وسیله مناسبی جهت نفوذ اخلالگران به شبکه‌ها شده است.

اخلالگران رایانه‌ای دارای اهداف گوناگونی هستند، برخی با هدف کسب پول و سود به

1. Cyber Terrorism
2. Hackers

شبکه‌ها نفوذ می‌کنند و مثلاً با هک کردن کارت‌های اعتباری[1]، پول سرشاری به جیب می‌زنند، بعضی دیگر هدفشان سرگرمی، تفریح و به رخ کشیدن توان فنی و رایانه‌ای‌شان است، اما بسیاری از هکرها هم، دارای گرایشات سیاسی و یا اجتماعی هستند، به این گروه از هکرها Activities گفته می‌شود. هدف عمده این گروه از نفوذکننده‌ها، اخلال در سیستم‌های رایانه‌ای سازمان‌ها، وزارتخانه‌ها یا شبکه‌های مرتبط با دولت خاصی است. شبکه رایانه‌ای ارتش، وزارت دفاع، وزارت خارجه، پلیس، کاخ ریاست‌جمهوری، شبکه‌های رادیو و تلویزیون، بانک مرکزی، احزاب سیاسی، پارلمان و کنگره و سایر دستگاه‌های سیاسی از عمده‌ترین اهداف Activities یا نفوذگران رایانه‌ای سیاسی به‌شمار می‌روند. یکی از شگردهای اخلالگران رایانه‌ای، «خودداری از ارائه خدمات»[2] است. در این شیوه دستگاه مورد هدف، آنقدر با نامه‌های الکترونیک بمباران می‌شود که عملاً، توانایی خود را از دست داده و توان رایانه‌ای خود را برای ارائه خدمات از دست می‌دهد. «اتفاقی که در طول جنگ بالکان برای پایگاه‌های رایانه‌ای سازمان ناتو افتاد و آنقدر توسط نامه‌های الکترونیک مخالفان جنگ، بمباران شد که عملاً از کار افتاد».(۵)

وینستون چرچیل در جنگ جهانی دوم از پیدایش جنگ الکترونیک به‌عنوان «نبرد جادویی» نام برد و اینک پس از ۵۵ سال از آن گفتار، نبرد جادویی در عرصه اینترنت تحقق یافته است. به موازات آنکه دولت‌ها و شرکت‌ها سعی می‌کنند تا هرچه بیشتر شبکه‌های رایانه‌ای را تحت نفوذ و کنترل خود درآورند، شبکه اینترنت هم به محیطی مناسب برای تروریست‌های رایانه‌ای، فعالان سیاسی[3] و نفوذگران اینترنتی[4] و حتی خود دولت‌ها تبدیل شده است. Activist (نامی که به نفوذگرایان رایانه‌ای دارای گرایش‌های سیاسی و اجتماعی اطلاق می‌شود) شبکه رایانه‌ای ایالات‌متحده و شبکه‌هایی را که توسط اداره فدرال بازرسی ارتش اداره می‌شوند، تخریب کردند.

---

1. Credit Cards
2. Denial of Services
3. Political Activities
4. Hackers

نفوذگران رایانه‌ای در سال‌های اخیر به‌طور مستمر وارد پایگاه‌های اینترنتی سیاسی و اجتماعی شده‌اند و ضمن تغییر اطلاعات موجود در آنها به تبلیغ اعتقادات متعصبانه خود پرداخته‌اند. تابستان گذشته نیز طرفداران دو آتشه چینی و تایوانی همزمان با اوج‌گیری تنش نظامی میان دو کشور، شبکه‌های رایانه‌ای طرف مقابل را مورد حمله قرار دادند. به‌نظر می‌رسد که بمباران پایگاه‌های رایانه‌ای سازمان ناتو به‌وسیله نامه‌های الکترونیکی و نیز ارسال پیام‌های ضدجنگ برای پایگاه‌های اینترنتی دولت‌ها در سراسر جهان، کار آن گروه از فعالان سیاسی باشد که در جنگ بالکان از صربستان حمایت می‌کردند. به گفته کارشناسان این صنعت، به‌طور حتم، انجام اقدامات غیرقانونی از این قبیل در سال‌های آتی افزایش خواهد یافت. بدین ترتیب، این‌گونه مشکلات رایانه‌ای، بخشی از آینده این صنعت خواهد بود. بنا بر پیش‌بینی برخی از کارشناسان، شبکه‌های رایانه‌ای به‌طور فزاینده به عرصه‌ای برای نظامیان و تروریست‌ها تبدیل خواهد شد.

در سال ۱۹۹۸، وزارت دادگستری و پلیس فدرال آمریکا به‌طور مشترک واحد جدیدی به نام «مرکز پشتیبانی زیرساخت ملی»[1] تشکیل دادند که وظیفه آن تقویت توان دفاعی ایالات‌متحده در مقابل تروریسم رایانه‌ای و سایر تهدیدات الکترونیک است.

در سال ۲۰۰۲ نیز گزارشی که برای ارائه در یک کنفرانس دولتی در خصوص نقض امنیت رایانه‌ای[2] تهیه شده بود، بر این نکته تأکید داشت که حملات انجام گرفته به زیرساخت‌های اساسی، می‌تواند به‌صورت مستقیم و یا غیرمستقیم از طریق تأثیرات جانبی خود، موفقیت برنامه‌های ملی را با اشکال روبرو سازد و یا اینکه می‌تواند نشانه مقاصد شوم دولت‌ها یا تروریست‌های خارجی باشد. برای ایالات‌متحده که یکی از رایانه‌ای‌ترین کشورهای جهان محسوب می‌شود، پیشرفت‌های اینترنتی به مثابه شمشیر دولبه بوده است. این شبکه رایانه‌ای جهانی از یک‌سو زمینه رشد اقتصادی این کشور و تسهیل ارتباطات و فعالیت‌های تجاری

1. National Infrastructure Protection Center
2. To Break Computer Security

شرکت و افراد را فراهم ساخته و از سوی دیگر اقتصاد مبتنی بر اینترنت، این کشور را در مقابل تهدیدات رایانه‌ای آسیب‌پذیر کرده است.

به همین دلیل کاخ‌سفید برای پرداخت هزینه ایجاد سیستم حفاظت مخابراتی و ساخت زیرساخت‌های اساسی، درخواستی ۲ میلیارد دلاری را به کنگره ارائه داد. با این حال کارشناسان و بسیاری از اعضای کنگره آمریکا اعتقاد داشتند که این طرح نمی‌تواند برای حمایت از بخش خصوصی در مقابل حملات رایانه‌ای کار چندانی انجام دهد. حملاتی که به رایانه‌ها صورت می‌گرفت از نوع خودداری از ارائه خدمات[1] بود که موجب وارد شدن خسارت به توان رایانه برای اجرای دستورهای وارده می‌شود. همچنین این اعتقاد نیز وجود دارد که حملاتی که موجب از کار افتادن موقت رایانه‌های ناتو در جریان منازعه کوزوو شد، از این نوع بوده است.

مدتی بعد دو سرهنگ ارتش چین با انتشار کتابی به نام «جنگ نامحدود»[2] این موضوع را مطرح کردند که چین به‌منظور کسب توانایی جنگیدن با کشور قدرتمندی چون آمریکا، نیازمند یافتن شیوه‌هایی جدید و غیرمتعارف رویارویی همچون استفاده از تروریسم رایانه‌ای است. در سال ۲۰۰۲ نیز چندین پایگاه بین‌المللی اینترنتی متعلق به گروه مذهبی Falun Dafa چین، توسط نامه‌های الکترونیک و سایر سلاح‌های دیجیتال[3] مورد حمله قرار گرفتند. بسیاری از صاحبنظران مسائل رایانه‌ای و اینترنتی اعتقاد داشتند که این اقدامات از جانب دولت چین که در آن زمان حملاتی را علیه گروه مذکور آغاز کرده بود، رهبری شده است. در ماه اوت سال ۲۰۰۲ نیز چندین پایگاه دولتی رایانه‌ای تایوان، انباشته از پیام‌هایی شدند که همگی مخالفت خود را با دولت و استقلال این کشور اعلام می‌کردند. به‌دنبال آن، نفوذگران رایانه‌ای تایوانی وارد پایگاه‌های چینی شدند و سرود ملی تایوان و نیز پیام‌هایی را به طرفداری از این کشور انتشار دادند. به اعتقاد دست‌اندرکاران صنعت رایانه، حملات رایانه‌ای در هر مرحله‌ای که

1. Denial of Services
2. Unrestricted War
3. Digital Weapons

صورت بگیرد، موضوعی جدی برای امنیت ملی کشورها محسوب می‌شود. با این حال در وضعیت کنونی، چنین حملاتی را بیش از آنکه بتوان یک فاجعه قلمداد کرد، تنها باید عاملی برای تأخیر در انجام کارها و نوعی دردسر دانست.(۶)

۶ـ۱ـ اینترنت در خدمت تروریست‌ها

به‌رغم سخت‌گیری شدید دولت‌ها برای محدود و مسدود کردن منابع مالی تروریست‌ها و اصولاً فعالیت‌های آنها، اما همه روزه میلیون‌ها دلار مبادله مالی از طریق اینترنت بین این گروه‌ها و منابع تأمین‌کننده آنها و نیز نحوه ارائه دستورات لازم از سوی سران و فرماندهان این گروه‌ها به عوامل آنها در کشورهای مختلف صورت می‌گیرد.

رادیو مسکو در گزارشی پیرامون نحوه مبادلات مالی این گروه‌ها گفت: این مبادلات که از طریق اینترنت و به‌وسیله سفارش‌های دروغین کالا صورت می‌گیرد، دارای کدهای رمزی است که فقط اعضای آن گروه‌ها قادر به تشخیص آنها هستند. سفارش کالا، تحت عنوان یک شرکت تجاری از یک شرکت تجاری دیگر صورت می‌گیرد و نوع کالا و میزان هزینه آن مشخص می‌گردد در حالیکه در این میان، فقط پول است که به‌وسیله کارت‌های اعتباری رد و بدل می‌شود و از کالا هیچ خبری نیست. همچنین وجود سایت‌های اختصاصی این گروه‌ها بر روی اینترنت به آنها کمک می‌کند تا پیام‌ها، دستورالعمل‌ها و ریزبرنامه‌های فعالیت‌هایشان را به اعضا بدهند و برای اینکه شناخته نشوند و پایگاه‌هایشان توسط مأموران امنیتی کشف نشود، آدرس‌های اینترنتی[1] خود را به‌سرعت تعویض می‌کنند و اصولاً آدرس‌های اینترنتی واقعی ندارند.(۷)

تروریسم به استفاده از خشونت یا تهدید به استفاده از آن به قصد ارعاب یا وادارکردن جوامع و دولت‌ها به عمل یا تصمیم خاصی اطلاق می‌شود. عمل تروریستی می‌تواند توسط

---

1. Internet Addresses

افراد یا گروه‌ها انجام گیرد و انگیزهٔ آن غالباً اهداف ایدئولوژیکی یا سیاسی است. تروریست‌ها به‌طور سنتی از دو شکل اصلی جنگ اطلاعاتی یعنی جمع‌آوری اطلاعات و عملیات روان‌شناختی و مدیریت درک استفاده می‌کنند. تعدادی از گروه‌ها، برای پشتیبانی از این عملیات، استفاده از فناوری رایانه را آغاز کرده‌اند (مثلاً استفاده از اینترنت برای پخش تبلیغات و انواعی از منابع در خط ـ On line ـ برای جمع‌آوری اطلاعات). در فوریه ۱۹۹۸، کلارک استاتن[1]، مدیر اجرایی انستیتوی پژوهش و پاسخ اضطراری[2] در شیکاگو در یک کمیته سنای ایالات‌متحده شهادت داد که «اکنون حتی گروه‌های کوچک تروریستی نیز برای پخش پیام‌های خود و گمراه کردن مردم کشورهای مختلف به‌طور همزمان، از اینترنت استفاده می‌کنند». او نسخه‌هایی از پیام‌های داخلی و بین‌المللی را که حاوی تهدیدات و تبلیغات ضدآمریکایی و ضداسرائیلی بود، از جمله دعوت افراطی پخش شده به جهاد (جنگ مقدس) بر ضد آمریکا و بریتانیای کبیر را به آن کمیته تسلیم کرد. در ماه ژوئن، «اخبار ایالات‌متحده و گزارش جهان» یادآور شد که از ۳۰ گروهی که در بست سازمان‌های تروریستی وزارت دفاع ایالات‌متحده قرار گرفته‌اند، ۱۲ سازمان در شبکه حضور دارند که نمی‌توان آنها را با زور از شبکه بیرون کرد زیرا آنها قادرند در کشورهایی که دارای قوانین آزادی بیان هستند، سایت‌های خود را تأسیس کنند. مثلاً دولت سریلانکا، جدایی‌طلبان ببرهای آزادی‌بخش تامیل را غیرقانونی کرده و حتی تلاش نموده تا سایت آنها (که مرکزش در لندن است) را نیز تعطیل کنند.[(۸)]

گفته می‌شد که ارتش جمهوری‌خواه ایرلند قبل از قرارداد صلح ۱۹۹۸، «یک بانک اطلاعاتی هوشمند رایانه‌ای[3] با استفاده از بانک‌های اطلاعاتی جمهوری ایرلند، آمریکا و فرانسه» ایجاد کرده است. یک هوادار که کارمند تلکوم بریتانیا بود، سوابق صورت‌حساب‌های تلفن را سرقت کرد تا نشانی‌های اهداف بالقوه (برای کشته شدن) را تعیین کند. همچنین ارتش جمهوری‌خواه ایرلند نیز از طریق بانک‌های اطلاعاتی، نشانی‌های مشتریان شرکت‌های

---

1. Clark Staten
2. ERRI
3. Intelligent Cyber Information Banks

خصوصی مراقبت‌های بهداشتی BUPA و آژانس‌های مسافرتی «تامس کوک» را جست‌وجو می‌کرد. این شبکه اطلاعاتی، با فناوری بالا زمانی کشف شد که مقامات، تعدادی از دیسکت‌های رایانه‌ای را در بلفاست ضبط کردند. در این دیسکت‌ها، نسخه‌هایی از ثبت الکترونیکی که برای پیدا کردن نام مقامات پلیس و سایر هدف‌های بالقوه مورد استفاده قرار می‌گرفت، وجود داشت. ارتش جمهوری‌خواه ایرلند، برای مخفی نگاه داشتن فایل‌های خود از رمز استفاده می‌کرد، اما افسران توانستند پس از ماه‌ها تلاش، رمز دیسکت‌ها را کشف کنند.(۹)

سایر گروه‌های تروریستی نیز از رمزسازی[1] به‌عنوان یک وسیله جنگ اطلاعاتی دفاعی استفاده کرده‌اند. رمزی یوسف، مغز متفکر بمب‌گذاری مرکز تجارت جهانی در سال ۱۹۹۴ و بمب‌گذاری در یک هواپیمای خطوط هواپیمایی مانیلا در ۱۹۹۵، فایل‌هایی را که در رایانه کیفی خود ذخیره کرده بود، رمزسازی نموده بود. وقتی مقامات، رایانه او را در مانیل ضبط کردند و به رمز فایل‌هایی دست یافتند که اطلاعاتی درباره طرح‌های آتی او مانند منفجر کردن ۱۱ هواپیمای تجارتی متعلق به آمریکا در خاوردور را در دست اقدام داشت.(۱۰) همچنین، مواردی از اقدامات تروریستی نیز وجود داشت که در آنها به‌طور مستقیم به سیستم‌های مخابراتی و رایانه‌ای حمله شده است. مثلاً در دهه ۷۰، بریگادهای سرخ ایتالیا، علیه مؤسسات صنایع الکترونیک[2]، رایانه و تسلیحاتی ۲۷ حمله انجام دادند.(۱۱) شعار آنها برای انهدام سیستم‌ها و تأسیسات رایانه‌ای «ضربه زدن به قلب دولت» بود.(۱۲) حملات نرم‌افزاری[3] به سیستم‌های رایانه‌ای با ماهیت تخریبی را گاهی «تروریسم اطلاعاتی»[4] می‌نامند. نفوذهای رایانه‌ای که در فایل‌های رایانه‌ای خرابکاری می‌کند و آنها را پاک می‌نماید، رها ساختن عمدی ویروس در یک شبکه و حملات مبتنی بر رایانه که از راه دور، سرویس‌ها را مختل و رایانه‌ها را از کار می‌اندازد، از جمله اقدامات تروریسم اطلاعاتی است. اما، در اکثر موارد، این اقدامات توسط تروریست‌ها به مفهوم سنتی آن انجام نشده، بلکه توسط واردشوندگان غیرمجاز به

---

1. Cod'ing
2. Electronic Industrial Institute
3. Software Attacks
4. Information Terrorism

سیستم‌ها و کارکنان ناراضی انجام گرفته است. هدف آنها، یک سازمان خاص بوده، نه تمام کشور و اثر آنها نیز عمدتاً محدود به همان سازمان مورد حمله بوده و اقدامات آنان نیز با خشونت فیزیکی همراه نبوده است.

آنچه مقامات اطلاعاتی آمریکا آنرا اولین حمله شناخته‌شده تروریست‌ها به سیستم‌های رایانه‌ای یک کشور می‌دانند، چریک‌های قومی تامیل، هزاران پیام الکترونیکی را به سفارتخانه‌های سریلانکا ارسال کردند. در این پیام‌ها گفته شده بود: «ما ببرهای سیاه اینترنت هستیم و برای مختل کردن ارتباطات شما این کار را انجام داده‌ایم».(۱۳) یک شاخه منشعب شده از ببرهای تامیل که برای استقلال سرزمین خود برای اقلیت تامیل‌ها هستند نیز مشمول این واقعه بود.(۱۴)

بمباران با پست الکترونیکی، شامل ارسال ۸۰۰ پیام در روز به مدت دو هفته بود. ویلیام چرچ[1]، دبیر مرکز مطالعات جنگ زیرساختی[2]، معتقد بود که «ببرهای آزادی‌بخش تامیل از مشهور شدن ناامید هستند و دقیقاً آنچه را که می‌خواستند به‌دست آوردند ... با توجه به حملات مرگبار و عادی ببرها، اگر این نوع فعالیت‌ها آنها را از بمب‌گذاری و کشتن منحرف کند، مرکز مایل است آنها را به نام صلح تشویق کند تا بیشتر، به این نوع اقدامات تروریستی دست بزنند».(۱۵) اما، چنین حمله‌ای، این اثر مطلوب را داشت که در سفارتخانه‌ها ایجاد ترس کرد. این پیام‌ها می‌توانست پیش‌درآمد حملات مخرب‌تر بر رایانه‌ها، در اینترنت باشد.

در دهه ۸۰ م. باری کولین[3]، پژوهشگر ارشد انستیتوی اطلاعات و امنیت در کالیفرنیا، واژه «سایبر تروریسم»[4] را جعل کرد. این واژه جعل‌شده توسط او، سایبر ـ فضا و تروریسم را دربر می‌گرفت.(۱۶) مارک پولیتی، مأمور ویژه FBI یک تعریف کارساز برای آن واژه ارائه می‌دهد: «سایبر تروریسم، حمله از پیش طراحی‌شده و دارای انگیزه‌های سیاسی به سیستم‌های رایانه‌ای،

---

1. William Church
2. CIWARS
3. Barry Collin
4. Cyber Terrorism

برنامه‌های رایانه و داده‌ها است که به خشونت علیه اهداف غیرمتخاصم توسط گروه‌های زیرملی[1] یا عوامل پنهان، منجر می‌شود».(۱۷)

آیا سایبرتروریسم، روشی در آینده است؟ برای یک تروریسم، سایبر تروریسم بر روش‌های فیزیکی برتری‌هایی دارد، از جمله می‌تواند از راه دور انجام گیرد، هزینهٔ آن کم است و نیازی به حمل مواد منفجره در یک مأموریت انتحاری ندارد. احتمالاً پوشش گستردهٔ رسانه‌ها را به‌دست خواهد آورد، زیرا روزنامه‌نگاران[2] و مردم، عملاً مجذوب هر نوع حمله رایانه‌ای هستند. یکی از مطالعات مربوط به خطرات سیستم‌های رایانه‌ای که بسیار مورد تحسین قرار گرفت با پاراگرافی شروع می‌شد که با جمله زیر خاتمه می‌یافت: «تروریست‌های فردا ممکن است با یک صفحه کلید[3] کار بیشتری انجام دهند تا با یک بمب».(۱۸)

کولین[4] در جزوه‌ای که در سال ۱۹۹۷ نوشت، چند سناریوی احتمالی را شرح می‌دهد. در یک سناریو، یک سایبرتروریست[5] به سیستم کنترل فراوری یک کارخانه غلات وارد می‌شود و مقداری مکمل آهن را تغییر می‌دهد. تعدادی از بچه‌ها بیمار می‌شوند و می‌میرند. در رویدادی دیگر، سایبرتروریست‌ها به نسل بعدی سیستم‌های کنترل ترافیک هوایی حمله کرده و دو هواپیمای غول‌آسای غیرنظامی با هم تصادف می‌کنند. در سومین رویداد، سایبر تروریست‌های بانک‌ها، معاملات مالی بین‌المللی و بورس اوراق بهادار را دستخوش اختلال می‌سازند. در نتیجه، سیستم‌های اقتصادی دچار وقفه می‌شوند، مردم اعتماد خود را از دست می‌دهند و بی‌ثباتی به‌وجود می‌آید.(۱۹)

پولیت، درست بودن حملات فرضی کولین را مورد تجزیه و تحلیل قرار می‌دهد و نتیجه‌گیری می‌کند که در فرآیندهای کنترل که امروزه رواج دارد، نقش انسان تا آن حد کافی است که در حال حاضر سایبر تروریست‌ها می‌تواند برای مفهوم کلاسیک خود، خطر مهمی

---

1. Sub national
2. Journalists
3. Keyboard
4. Collin
5. Cyber Terrorist

ایجاد کنند. مثلاً در سناریوی آلوده کردن غلات، مقدار آهنی (یا هر ماده غذایی دیگر) که برای سمی کردن غلات نیاز داریم به حدی زیاد است که کارگران خط بسته‌بندی متوجه آن خواهند شد. آنها آهن را از خط تولید دور خواهند کرد و محصول طعم متفاوتی خواهد داشت و در نتیجه خوب نخواهد بود. در سناریوی کنترل ترافیک هوایی، انسان‌هایی که در مدار کار قرار دارند متوجه مسئله خواهند شد و اقدام اصلاحی به‌عمل خواهند آورد. او می‌گوید: خلبانان برای آگاهی از این وضعیت‌ها، پی بردن به اشتباهات کنترل‌کننده‌های ترافیک هوایی و چگونه عمل کردن در فقدان کلی کنترل ترافیک هوایی، آموزش دیده‌اند. البته تجزیه و تحلیل او به‌طور ضمنی نمی‌گوید که رایانه‌ها، ایمن و فارغ از هر نوع آسیب‌پذیری هستند. برعکس، استدلال او این است که به‌رغم این آسیب‌پذیری‌ها، چون انسان در مدار وجود دارد، بعید است یک حملهٔ سایبر، پیامدهای این‌چنین ویرانگری داشته باشد. او نتیجه‌گیری می‌کند به‌تدریج که فناوری‌های بیشتر و بیشتری وارد تمدن خود می‌کنیم، باید مطمئن شویم برای محافظت از افرادی‌که آن فناوری در خدمت آنها است، دخالت و نظارت کافی وجود دارد.[۲۰]

حداقل دو مطالعه مستقل نشان داده که سیستم‌های مالی، در برابر حمله جنگ اطلاعاتی توسط تروریست‌ها یا گروه‌های متخاصم دیگر، آسیب‌پذیر هستند. به موجب یکی از این مطالعات که توسط تام مانزی[۱] انجام گرفته، سیستم پرداخت بین بانکی پایاپای[۲] یا سیستم انتقال وجه فدوایر[۳] که توسط سیستم رزرو فدرال انجام می‌گیرد، ممکن است با یک حمله فیزیکی که در آن ترکیبی از بمب اتومبیل و سلاح‌های الکترومغناطیسی استفاده می‌شود، برای مدت زمانی طولانی از کار بازماند. مطالعه دیگر توسط ادوارد براون از نیروی هوایی انجام شده است. او استدلال می‌کند که سیستم‌ها، از نظر فیزیکی خود محافظت شده‌اند، اما سیستم پرداخت بین بانکی پایاپای در برابر حمله‌ای که از عقب ماندن روزانه بستانکاری‌ها در مقابل بدهی‌ها بهره‌برداری کند، آسیب‌پذیر است.[۲۱] بریان س. بایگلو[۴]، سروان نیروی هوایی ایالات‌متحده، هر دو سناریوی فوق را رد می‌کند

---

1. Tom Manzi
2. CHIPS
3. Fed Wire
4. Brian S. Bigelow

و استدلال می‌نماید که در این سیستم‌ها، کنترل‌ها و تعادل‌های اساسی وجود دارد. «هم سناریوی براون و هم سناریوی مانزی، باور غلطی را که اعتبار بسیاری از بحث‌های جنگ اطلاعاتی را تضعیف می‌کند، نشان می‌دهند. قابل انکار نیست که استفاده از رایانه‌ها و شبکه‌ها، آسیب‌پذیری ایجاد می‌کند اما اینکه گفته شود آنها پاشنهٔ آشیل زیرساخت‌های خدمات مالی هستند، نادیده گرفتن اقدامات بسیار قابل ملاحظه‌ای است که مؤسسات، برای مدیریت بر خطرهای سیستم‌های اطلاعاتی خود به‌عمل آورده‌اند».

سیستم‌های مخابرات متحمل حملات متعددی شده‌اند، اما تا به حال هیچ‌یک نتیجه‌ای بیش از سختی موقت نداشته‌اند، قطع ماهواره در مه ۱۹۹۸، نشانگر این واقعیت است. وقتی ماهواره شرکت پان ام ست[1] در بعدازظهر روز سه‌شنبه ۱۹ مه از کنترل خارج شد بسیاری از سرویس‌های پیجینگ ایالات‌متحده و پاره‌ای از تغذیه‌های داده‌ها و رسانه‌ها فلج شد. شرکت، بلافاصله شروع به انتقال سیگنال‌ها به ماهواره‌های دیگر پان‌ام‌ست کرد و پزشکان، پرستاران و افسران پلیس به فناوری‌های دیگری مانند بی‌سیم‌های دستی، رادیوهای قابل حمل و تلفن‌های سیار رو آوردند. رادیوی محلی عمومی شروع به پخش «همه چیز تحت بررسی است»، از خطوط تلفن کرد و به سایت خود در شبکه، صوت واقعی[2] تغذیه کرد. تا صبح پنج‌شنبه، ۷۵ درصد کارهایی که به ماهواره مزبور بستگی داشت به پهنای باندهای دیگر واگذار شده بودند. پیج نت[3] که بزرگ‌ترین سرویس پیج در کشور است، می‌گوید که ۸۵ درصد از ۱۰/۴ میلیون مشتری آن، تا پنج‌شنبه دارای بوق‌زنندهٔ فعال شده بودند و سایرین نیز تا جمعه، عملیاتی می‌گردیدند. به نوشتهٔ واشنگتن تایمز، «هیچ‌گونه گزارشی دال بر اینکه به‌علت از کار افتادن ماهواره، کسی آسیب جدی دیده، واصل نشده است. در وال‌استریت هیچ فریادی درباره از دست رفتن معاملات شنیده نشد».(۲۲)

ویلیام چرچ در مقاله‌ای با عنوان «چند تروریست در پشت صفحه کلید رایانه، مناسب

1. Pan Am sat corp
2. Real Audio
3. Page Net

هستند؟» حالت نیرومندی ارائه می‌دهد و می‌گوید: «ایالات‌متحده، تا به حال با یک تهدید مجبورکننده از ناحیه تروریست‌ها که با استفاده از تکنیک‌های جنگ اطلاعاتی برای از کار انداختن زیرساخت‌های حساس انجام شده باشد روبرو نبوده است.(۲۳) در این زمان، تروریست‌ها برای انجام یک حمله سایبر، انگیزه، توانمندی یا مهارت ندارند.» چرچ، امکان حمله فیزیکی به زیرساخت‌ها را منتفی نمی‌داند، اما این تهدید، نه تازه است و نه با تکیه ایالات‌متحده به فناوری، تشدید شده است. چرچ در مقاله دیگری، تروریست‌ها را در فهرست تهدیدات جنگ اطلاعاتی علیه ایالات‌متحده قرار می‌دهد. تهدیدات مزبور به ترتیب نزولی، عبارتند از جرائم سازمان‌یافته (کلاهبرداری مالی و اخاذی)، تروریسم فردی، ورود غیرمجاز به سیستم، سازمان‌های غیردولتی دارای جهت‌گیری‌های اساسی، گروه‌های تروریستی از نظر فیزیکی خشن و بالاخره سایر دولت‌ها. کلارک استاتن[1] تأیید می‌کند که باور بر این بود که «اعضای پاره‌ای از سازمان‌های افراطی اسلامی کوشیده‌اند برای حمایت از فعالیت‌های رایانه‌ای خود و حتی انجام حملات جنگ اطلاعاتی تهاجمی[2] در آینده، یک «شبکه ورود غیرمجاز به سیستم‌ها»[3] ایجاد کنند.(۲۴)

شواهد اولیه، حاکی از آن است که امکان دارد گروه‌های تروریستی برای نفوذ در درک مردم و هماهنگ کردن فعالیت‌های خود برای انجام حملات مخرب و مختل کننده خود، حداقل علیه خود شبکه از اینترنت استفادهٔ بیشتری بکنند. احتمالاً زمانی که اینترنت به‌صورت عملیاتی فعال شد برای آنها ارزش بیشتری پیدا می‌کند. اگر چنین شود به نفع کسانی خواهد بود که زیرساخت‌های پشتیبان مانند آنچه برای مخابرات و برق لازم است را در اختیار داشته باشند.(۲۵)

در حال حاضر، خطر تروریست‌ها به‌خاطر بمب‌ها و سلاح‌های کشتارجمعی، مخصوصاً سلاح‌های شیمیایی و میکروبی، بزرگ‌تر از خطر حملات سایبر[4] شده است. اثر این نوع حملات احتمالاً خشن‌تر و اثر روان‌شناختی آن بیشتر از چیزی است که در سایبر فضا می‌توان

---

1. Crack Staten
2. Offensive Information Warfare
3. Illegal Network for Entrance to System
4. Cyber attacks

تصور کرد.(۲۶) به‌علاوه، حملات سایبر با عدم قطعیت بیشتری همراه هستند. پیش‌بینی خسارات ناشی از بمبی که خوب کار گذاشته شده باشد از پیش‌بینی خسارات ناشی از قطع سرویس‌های رایانه‌ای، رها کردن ویروس، یا دستکاری در پرونده‌های الکترونیکی[1]، آسان‌تر است. تا به‌حال، مخرب‌ترین حملات توسط واردشوندگان غیرمجازی که شیطنت می‌کنند یا به سیاست‌ها معترضند و همچنین توسط اشخاصی که درصدد انتقام از کارفرمای قبلی خود هستند، انجام گرفته، اما هیچ‌یک از این حملات با مرگ‌ومیر همراه نبوده است.(۲۷)

حملات سایبر می‌تواند به‌عنوان وسیله کمکی، جهت حمایت از عملیاتی دیگر مورد استفاده قرار گیرد، مثلاً به‌عنوان پشتیبان عملیات نظامی متعارفی (و نه به‌عنوان جانشین آنها) انجام گیرند. برای روشن شدن موضوع به مورد زیر اشاره می‌کنیم. در اوایل سال ۱۹۹۸، یک عیب طراحی در سیستم برچسب امنیتی که به‌طور گسترده‌ای مورد استفادهٔ فرودگاه‌ها، زندان‌های ایالتی، مؤسسات مالی، پیمانکاران ارتش، ادارات دولتی (از جمله سیا) و شرکت‌های برخوردار از فناوری بالا قرار داشت، گزارش شد.(۲۸) این آسیب‌پذیری به متجاوز امکان می‌داد از یک ارتباط شبکه‌ای[2] یا تلفنی برای ایجاد برچسب دائمی یا موقت که موجب دسترسی به مناطق مورد نظر امنیتی، مناطق حساس محافظت از درهای بدون قفل، رویدادهای برنامه‌ریزی شده مانند باز کردن تمام درها در زمان معین می‌شد، استفاده نماید و برچسب‌هایی طراحی کند که از ورود و خروج شخص به منطقه مورد نظر امنیتی، هیچ نشانه‌ای باقی نگذارد. می‌توان یک گروه تروریست را در نظر مجسم کرد که به‌عنوان بخشی از یک عملیات بزرگ‌تر و به‌منظور نفوذ در امنیت فرودگاه‌ها، می‌کوشند از این آسیب‌پذیری بهره‌برداری نمایند. پس از آن، می‌توان مواد منفجره را در داخل یک هواپیما مخفی کرد.(۲۹)

هیچ‌کدام از این مطالب مدعی نمی‌شود که حمله فاجعه‌بار سایبر نمی‌تواند روی دهد و روی نخواهد داد. آینده را نمی‌توان پیش‌بینی کرد و ممکن است حمله‌ای به‌صورتی که

---

1. Electronic Files

2. Network Communication

پیش‌بینی نشده، انجام گیرد. بنابراین، شایسته است برای اطمینان یافتن از اینکه زیرساخت‌های اساسی به حد کافی در برابر هر اقدام خصمانه‌ای، چه از ناحیهٔ تروریست‌ها باشد یا از ناحیه دولت‌های خارجی، وارد شوندگان غیرمجاز[1]، یا دزدان دارای فناوری بالا[2]، مستحکم باشند و مقاومت کنند، اقدامات لازم انجام گیرد. همچنین، طراحی سناریوهایی مانند آنچه کولین، مانزی، براون و سایرین ساختند، دارای ارزش است، زیرا برای کشف و تجزیه و تحلیل تهدیدها و آسیب‌پذیری‌های بالقوه، ابزار نیرومندی در اختیار می‌گذارند.[۳۰]

۷ـ۱ـ صحنه‌های جدید

در همان زمانی که آرکوئیلا[3] و رانفلرت[4]، برای اندیشیدن درباره عملیات نظامی بر طبق اصول مرتبط با اطلاعات، واژه جنگ سایبر را ارائه دادند، برای فکر کردن به مبارزات مرتبط با اطلاعات که غالباً با نبرد کم‌شدت بازیگران غیردولتی (مانند سازمان‌های غیردولتی) همراه است، واژه جنگ شبکه‌ای را نیز ارائه دادند.[۳۱] آنها پیش‌بینی می‌کنند که مبارزات آینده توسط گروه‌هایی انجام خواهد شد که بیشتر به‌صورت شبکه سازماندهی شده‌اند تا به‌صورت سلسله مراتب. همچنین استدلال می‌کنند که شبکه‌ها می‌توانند سازمان‌ها را مغلوب کرده و سلسله مراتب، برای جنگیدن با شبکه‌ها را مشکل سازند، به‌ویژه به «شبکه‌های تمام کانال»[5] که در آنها هر گره[6] را می‌توان به گره دیگری متصل نمود، توجه نشان می‌دهند. این نوع شبکه، رشد طبیعی فناوری‌های مدرن، به‌خصوص اینترنت است و ارتباط آسان بین دو موجودیت را ممکن می‌سازد. آرکوئیلا و رانفلرت معتقدند که شکل شبکه، یکی از مهم‌ترین آثار تکامل اطلاعات در تمام قلمروها (سیاسی، اقتصادی و اجتماعی) می‌باشد. قدرت به سوی افرادی مهاجرت خواهد کرد که می‌توانند به آسانی، شبکه‌های گسترده‌ای را سازمان دهند. «آینده ممکن است به افرادی تعلق داشته باشد که به‌صورت شبکه مسلط هستند».[۳۲]

---

1. Illegal Persons
2. High Technology Thefts
3. Arcouila
4. Ranflert
5. Full Channel Network
6. Node

همانند جنگ سایبر، در جنگ شبکه‌ای نیز از انواع سلاح‌های فنی و غیرفنی استفاده می‌شود. در عملیات سعی می‌شود آنچه را که جمعیت هدف، درباره خود و دنیای پیرامون خود می‌داند یا تصور می‌کند که می‌داند مختل کند، آسیب ببیند یا تغییر دهد. در جنگ شبکه‌ای[1]، عملیات روان‌شناختی و مدیریت درک از جمله اقدامات دیپلماسی عمومی، تبلیغاتی، براندازی فرهنگی و سیاسی، فریب رسانه‌های محلی یا نفوذ در آنها و تلاش برای تقویت جنبش‌های ناراضیان یا مخالفان از طریق شبکه‌های رایانه‌ای وجود دارد. همچنین در جنگ‌های شبکه‌ای، از فناوری‌های اطلاعات بهره‌برداری می‌شود و حتی ممکن است شامل نفوذ در شبکه‌های رایانه نیز باشد. جنگ شبکه‌ای ممکن است بین دولت‌های کشور ـ ملت‌های رقیب، توسط دولت‌ها علیه گروه‌های فعال در تروریسم، موادمخدر، یا تکثیر سلاح‌های کشتارجمعی و همچنین توسط گروه‌های سیاسی علیه دولت‌ها انجام گیرد.(۳۳)

یک نمونه جنگ شبکه‌ای را می‌توان در مبارزه ارتش آزادی‌بخش ملی زاپاتیستا[2] و دولت مکزیک یافت. در اولین روز سال ۱۹۹۴، ارتش آزادی‌بخش ملی زاپاتیستا، ۶ شهر را در چیاپاس اشغال کردند و علیه دولت مکزیک، اعلان جنگ نمودند، خواهان تغییراتی شدند و سرانجام به یک پیکار رسانه‌ای جهانی دست زدند. آنها بیانیه‌های مطبوعاتی صادر می‌نمودند، از خارجیان دعوت می‌کردند به چیاپاس آمده و وضعیت را به چشم خود ببینند و در این بین کنفرانس‌هایی ترتیب دادند. آنها خواهان اصلاحات سیاسی، اقتصادی و اجتماعی از جمله حقوقی برای بومیان، انتخابات مشروع و منصفانه، لغو مقررات حاکم بر اجاره زمین (مصوب ۱۹۹۲) و مردم‌سالاری سیاسی واقعی شدند. ارتش مکزیک، سرزمین‌های اشغالی را پس گرفت، اما زاپاتیستاها سعی کردند، از دارا نبودن زاپاتیستاها و حامیان آنها از اینترنت برای سخن گفتن دربارهٔ وضعیت خود و هماهنگ کردن فعالیت‌ها استفاده کنند. یک گروه از حامیان نیویورکی، به نام تأتر مزاحمت الکترونیکی[3]، حمله به سایت زدیلو[4]، رئیس‌جمهور مکزیک، را

1. Network Warfare
2. EZLN
3. EDT
4. Zedillo

سازمان دادند. در ۱۰ آوریل ۱۹۹۸، شرکت‌کنندگان در حمله، بروزرهای[1] شبکه وب خود را به سایتی با نرم‌افزار فلاد نت[2] که سایت هدف را با ترافیک بمباران می‌کرد، وصل کردند. تأتر مزاحمت الکترونیکی، برنامه‌ریزی کرد که در ۱۰ مه، حمله را تکرار کند، اما وقتی گروه حقوق‌بشر مستقر در مکزیک (AMELAPAZ یعنی صلح را دوست بدارید) اعتراض نمود، برنامهٔ خود را تغییر داد. این گروه حقوق‌بشر به هر نوع حمله‌ای که قانون را نقض می‌کرد، معترض بودند: «روشن است که در اینترنت جنگی وجود دارد که زاپاتیستاها در حال برنده شدن هستند ارتش آزادی‌بخش ملی زاپاتیستا پیشنهاد نمی‌کند یا نمی‌خواهد که جامعه مدنی پشتیبان آن، اقدامات غیرقانونی انجام دهد». در پاسخ، تأتر مزاحمت الکترونیکی، طرح‌های خود را مورد تجدید نظر قرار داد و در عوض به سایت کاخ‌سفید (کلینتون) حمله کرد. پس از این کار، زاپاتیستاها از این حمله فاصله گرفتند.

در ۹ سپتامبر، تأتر مزاحمت الکترونیکی دوباره به سایت پرزیدنت زدیلو و نیز سایت‌های پنتاگون و بورس فرانکفورت حمله کرد. حملات شبکه‌ای با جشنوارهٔ آرس الکترونیکا در جنگ اطلاعاتی که در لیز اتریش برگزار می‌شد، همزمان بود. به گفتهٔ برت استالبائوم[3]، طراح نرم‌افزار فلاد نت که در حمله مورد استفاده قرار گرفت، علت انتخاب پنتاگون این بود که «ما معتقدیم ارتش ایالات‌متحده، سربازانی را که حقوق‌بشر را نقض می‌کنند، آموزش داده است». استالبائوم گفت که علت انتخاب بورس فرانکفورت این بود که این بورس، مظهر جهانی شدن است و جهانی شدن، ریشهٔ مشکلات چیاپاس است. تأتر مزاحمت الکترونیکی، برآورد کرد که تا ده هزار نفر در تظاهرات شرکت کردند و در هر دقیقه، ۶۰۰,۰۰۰ بار کلید زدن، به هر کدام از این سایت‌ها وارد می‌شد، اما سرورهای مورد استفاده پنتاگون و دولت مکزیک ضربه را بازگرداندند. وقتی آنها یک حمله از سرورهای فلادنت را حس کردند در بروزرهای کاربران، دریچه بعد از دریچه باز کردند و در مواردی معترضان مجبور شدند، رایانه‌های خود را مجدداً

1. Browsers
2. Flood Net
3. Brett Stalbaum

راه‌اندازی کنند. بورس فرانکفورت نیز اعلام کرد که معمولاً شش میلیون کلیدزنی در روز دریافت می‌کند و به‌نظر می‌رسد سرویس‌ها آسیبی ندیده‌اند.

این مثال، این نظر را که اینترنت به‌عنوان وسیله نفوذ در افکار عمومی و فعالیت‌های هماهنگ‌سازی ارزشمندتر است تا برای عملیات مخرب، بیشتر مورد تأیید قرار می‌دهد.

۸ـ۱ـ حفظ زیرساخت‌های ملی

دولت ایالات‌متحده برای دفاع از زیرساخت‌های ملی، گام‌های متعددی برداشته است. اگرچه پرداختن به تمام آن گام‌ها از دامنه این کتاب خارج است اما دو مورد، ارزش مطرح شدن دارد. گام اول، تأسیس یک مرکز هماهنگی تیم پاسخ اضطراری رایانه‌ای[1] در دانشگاه کارنگی ـ ملون است. این مرکز، در ۱۹۸۸ پس از آنکه یک رویداد مهم در اینترنت، هزاران رایانه را دستخوش اختلال کرد، تأسیس شد. ادارهٔ پروژه‌های پیشرفتهٔ وزارت دفاع که اینترنت را بنا نهاد، مرکز هماهنگی تیم پاسخ اضطراری رایانه‌ای را طوری بنیان نهاده که ایالات‌متحده برای رویدادهای آتی بهتر آماده باشد. مرکز فوق دارای یک نقطه تماس ۲۴ ساعته و یک نقطه مرکزی برای مشخص کردن آسیب‌پذیری‌ها و رفع آنها به کمک فروشنده است.(۳۴)

از زمان تأسیس مرکز هماهنگی تیم پاسخ اضطراری رایانه‌ای، چندین مرکز پاسخ و پرداختن به رویدادها، در دولت فدرال تشکیل شده است. توانمندی‌های مشورتی رویداد رایانه‌ای وزارت نیرو[2] و ASSIST ادارهٔ سیستم‌های اطلاعاتی دفاعی از جملهٔ این مراکز هستند. در۱۹۸۹، تریبون تیم‌های امنیت و پاسخ به رویدادها[3] تأسیس شد تا مبادلهٔ اطلاعات و هماهنگی بین این مراکز تسهیل شود. این تلاش‌ها به تأسیس مرکز پاسخ به رویدادهای رایانه‌ای فدرال[4] منجر گشت. این مرکز براساس اشتراک، توانمندی پاسخ به رویداد در سطح یک دولت را تأمین می‌کند.

---

1. CERT/CC
2. CIAC
3. FIRST
4. Fed CIRC

گام دوم، تشکیل کمیسیون ریاست‌جمهوری درباره حفاظت زیرساخت‌های اساسی[1] در ژوئیه ۱۹۹۶ است. از این کمیسیون خواسته شد آن گروه از زیرساخت‌های حساس که سیستم‌های حمایت از جان را تشکیل می‌دهند، مطالعه کنند و آسیب‌پذیری‌های آنها را در برابر گسترهٔ وسیعی از تهدیدها مشخص نمایند و برای محافظت از آنها در آینده، راهبردی پیشنهاد کنند، بنابراین ۸ زیرساخت زیر مشخص شد که عبارتند از: مخابرات، بانکداری و مالیه، نیروی برق، توزیع نفت و بنزین و ذخیره آنها، تأمین آب، حمل‌ونقل، خدمات اضطراری و خدمات دولتی. کمیسیون، در گزارش نهایی خود که در دسامبر ۱۹۹۷ منتشر شد، اعلام کرد تهدیداتی که متوجه زیرساخت‌های اساسی واقعی هستند، از طریق وابستگی متقابل و ارتباط متقابل، ممکن است به نحو جدیدی آسیب‌پذیر گردند. بهره‌برداری عمدی از این زیرساخت‌های جدید ممکن است برای اقتصاد، امنیت و طراز زندگی ما پیامدهای جدی داشته باشد.[۳۵]

کمیسیون ریاست‌جمهوری دربارهٔ حفاظت زیرساخت‌های اساسی متوجه شد که تهدیدات سایبر[2]، منظره را تغییر داده است. «در گذشته ما به واسطه اقیانوس‌های پهن و همسایگان دوست، در برابر حملات خصمانه محافظت می‌شدیم، اما امروزه، تکامل تهدیدات سایبر، وضعیت را دستخوش تغییرات عمیقی کرده است. در سایبر، مرزهای ملی دیگر اهمیت سابق را ندارند. الکترون‌ها نمی‌ایستند که گذرنامه نشان دهند. حملات بالقوه جدی سایبر را می‌توان بدون آمادگی‌های لجستیکی قابل کشف، برنامه‌ریزی و اجرا کرد، همچنین می‌توان آنها را به‌طور نامرئی اکتشاف نمود، به‌طور پنهان تمرین کرد و سپس ظرف چند دقیقه یا حتی چند ثانیه بی‌آنکه هویت و محل حمله‌کننده مشخص شود، اجرا نمود».[۳۶]

کمیسیون مزبور در ارزیابی خطر حملات فیزیکی و حملات سایبر، چنین نتیجه‌گیری کرد که وسایل فیزیکی بهره‌برداری از آسیب‌پذیری‌های فیزیکی احتمالاً نگران‌کننده‌ترین تهدید زیرساخت‌های امروز ما باقی خواهند ماند. اما تقریباً تمام گروه‌هایی که ما با آنها گفت‌وگو نمودیم از تهدیدها و آسیب‌پذیری‌های جدید سایبر، اظهار نگرانی کرده‌اند. آنها بر اهمیت

---

1. PCCIP

2. Cyber Threats

تعیین رویکردهای معین به‌منظور حفظ زیرساخت‌ها در برابر تهدیدات سایبر تأکید داشتند و معتقد بودند، این کار باید قبل از تحقق یافتن تهدیدات و وارد آمدن خسارات عظیم بر سیستم‌ها، انجام گیرد. توصیه‌های کمیسیون ریاست‌جمهوری درباره حفاظت زیرساخت‌ها و ابتکارات بعدی، مانند تأسیس مرکز ملی حفاظت زیرساخت‌ها[1] و مرکز تصمیمات دفتر ریاست‌جمهوری[2]، در فصل آخر این کتاب خلاصه شده است.

اینکه سیستم‌های حساس به‌طور بالقوه در معرض حملات سایبر قرار دارند با تمرین ژوئن ۱۹۹۷ (تمرینی با اسم رمز «دریافت‌کنندهٔ خوانا» که توسط ادارهٔ امنیت ملی برگزار شد) مورد توجه قرار گرفت. تعیین آسیب‌پذیری‌های رایانه‌های ارتش ایالات‌متحده و پاره‌ای از زیرساخت‌های غیرنظامی در برابر یک حملهٔ سایبر، هدف این تمرین بود. بنا بر گزارش‌ها، تیمی مرکب از دو عضو، بخش‌های معینی از زیرساخت‌های نظامی از جمله، فرماندهی ایالات‌متحده در اقیانوس آرام (مستقر در هاوایی که به صد هزار نیروی آمریکایی در آسیا نظارت دارد) را هدف قرار دادند. یک نفر، نقش مهاجم را بازی کرد و نفر دیگر، کار را زیر نظر داشت تا مطمئن شود که طبق برنامه انجام می‌گیرد. این واردشوندگان ادارهٔ امنیت ملی، فقط با استفاده از ابزارهای فراوان و رایج ورود غیرمجاز که به آسانی از اینترنت قابل تحصیل است به تعدادی از سیستم‌ها، دسترسی ممتاز یافتند. آنها نتیجه گرفتند که زیرساخت‌های نظامی را می‌توان مختل کرد و آرایش احتمالی نیروها را با مانع روبرو ساخت. این تمرین، همچنین شامل سناریوهای مدونی علیه شبکه برق و سیستم اورژانس ۹۱۱ که موجب اخلال در این خدمات می‌گردد، نیز بود. در مورد اخیر، آنها به این نتیجه رسیدند که اگر به کاربران اینترنت، ایمیل‌های کافی فرستاده شود و در این پیام‌های پست الکترونیکی به آنها گفته شود که سیستم ۹۱۱ مشکلی دارد، تعداد زیادی از افراد کنجکاو فوراً به ۹۱۱ تلفن می‌کنند و در نتیجه سیستم با مشکل بار اضافی مواجه می‌شود. در این تمرین، علیه زیرساخت‌های غیرنظامی، حمله‌ای انجام نگرفت.[۳۷]

1. NIPC 2. PDD

۹ـ۱ـ جنگ اینترنتی و جنگ مجازی[1]

کارشناسان فناوری اطلاعات IT عقیده دارند، در جنگ‌های آینده، گروه‌های کوچک نظامی که با استفاده از آخرین تجهیزات اطلاعاتی و ارتباطی در جنگ‌ها شرکت می‌کنند، می‌توانند ارتش‌های تا دندان مسلح به سلاح‌های جنگی را از پای درآورند. در واقع، نیروهای نظامی عصر اطلاعات[2] با بهره‌گیری از اطلاعات به موقع و دقیق از موقعیت و برنامه‌های دشمن، به دانش برتر برای اهداف استراتژیک خود دست می‌یابند و با این ابزار قوی قادر به شناسایی دقیق نقاط قوت و ضعف طرف متخاصم و تصمیم‌گیری سریع در مورد نحوه حمله به آن خواهند بود. بررسی تاریخ در زمینه ارتش‌ها و چگونگی نبرد آنها در دوران مختلف نشان می‌دهد که آموزش‌ها، سازماندهی و استراتژی نظامی و جنگی آنها همواره در مواجهه با فناوری‌های جدید دچار نوعی چالش و تحول شده است. در جنگ جهانی اول، بروز انقلاب صنعتی باعث شکل‌گیری جنگ‌های فرسایشی[3] و ایجاد ارتش‌های بزرگ و مجهز شد، اما پس از حرکت کردن به سمت مکانیزه شدن، جنگ جهانی دوم جولانگاه سلاح‌های کشتارجمعی و تجهیزات مدرن و پیشرفته جنگی شد. انقلاب اطلاعاتی حاکی از ظهور نوعی تازه و متفاوت از عملیات جنگی است که در آن وسعت ارتش‌ها، قابلیت تحرک آنها و سلاح‌های پیشرفته کشتارجمعی نقش اصلی را بازی نمی‌کنند، بلکه برخورداری از اطلاعات بیشتر، توان رزمی و تاکتیکی ارتش‌ها را مشخص می‌سازد و میزان موفقیت آنها در میدان نبرد را تعیین خواهد کرد. به بیان دیگر، بهره‌مندی از اطلاعات کامل‌تر، دقیق‌تر و به موقع‌تر باعث می‌شود تا یک نیروی نظامی، قادر به سردرگم کردن دشمن و ضربه زدن به نقاط حساس آن شود. یکی دیگر از تأثیرات انقلاب اطلاعاتی[4] بر پدیده جنگ، تحول در عوامل و دلایل شکل‌گیری جنگ‌ها است. امروزه نحوه جمع‌آوری، پردازش و انتقال اطلاعات[5] باعث بروز تغییرات عمده‌ای در ساختار

1. Net War and Cyber War
2. Information Age
3. Attritive Wars
4. Information Revolution
5. Information Transfer

جوامع شده و بسیاری از سازوکارهای سنتی و رایج آنها را به چالش طلبیده است. همین امر موجب گشته تا قدرت از حالت متمرکز و انحصاری خارج شده و به نفع بازیگران کوچک‌تر و ضعیف‌تر تجزیه شود. به همین جهت بخش قابل توجهی از جنگ‌های آینده ناشی از چالش مذکور خواهد بود. علاوه بر آن، جنگ‌های عصر اطلاعات از طبقه‌بندی خاصی نیز برخوردارند. بخشی از آنها، جنگ‌های اینترنتی (Net Wars) خواهند بود که در واقع به‌نوعی ناشی از تضادهای اجتماعی است که عرصه آنها محیط سایبر اسپیس[1] می‌باشد و بخش دیگر جنگ‌های عصر اطلاعات، جنگ‌های مجازی و اطلاعاتی Cyber Wars هستند که در سطح ارتش‌ها رخ می‌دهند.

در جنگ اینترنتی که ممکن است بین ملت‌ها و جوامع رخ دهد دیپلماسی، تبلیغات، مبارزات روان‌شناسی، انهدام و ترور شخصیتی، سیاسی و تهاجم فرهنگی مطرح است. در واقع جنگ اینترنتی[2] معرف یک عصر تازه در طیف اختلافات و تضادهایی است که اشکال اقتصادی، سیاسی، اجتماعی و نظامی را دربرمی‌گیرد و هدف عمده آن، نابودی و یا اختلال در اطلاعات و ارتباطات است.[۳۸]

به عقیده نظریه‌پردازان، جنگ‌های اینترنتی[3] به اشکال مختلفی بروز خواهند کرد و برخی از آنها احتمالاً بین دولت‌های رقیب به وقوع خواهند پیوست. برخی دیگر نیز ممکن است دولت‌ها و عوامل غیردولتی را درگیر نمایند که بیشتر در حوزه فعالیت‌های تروریستی، قاچاق موادمخدر و یا تولید و توزیع سلاح‌های کشتارجمعی خواهد بود.

پس از اتمام جنگ آمریکا و انگلستان علیه عراق، وزارت امورخارجه آمریکا اقدام به راه‌اندازی یک سایت اینترنتی به زبان فارسی نموده که هدف آن «به اصطلاح ایجاد پلی میان آمریکا و ایران» است.[۳۹] این سایت که به‌طور رسمی سخنگوی وزارت خارجه آمریکا محسوب می‌شود در راستای جنگ روانی علیه ایران راه‌اندازی شده و در کنار سایت‌های فارسی زبان رادیو

---

1. Cyber Space
2. Net War
3. Net Wars

آمریکا[1] و رادیو فردا (شکل اصلاح‌شده رادیو آزادی که از پراگ برنامه پخش می‌کرد) عملاً بخش‌هایی از یک جنگ اینترنتی علیه ایران را راهبری می‌کند. جنگ اینترنتی می‌تواند مقدمه جنگ واقعی باشد، اما در جنگ‌های مجازی[2]، تنها عملیات نظامی براساس اصول و قواعد مبتنی بر اطلاعات صورت می‌گیرند. این جنگ‌ها، سیستم‌های اطلاعاتی و ارتباطی را نابود کرده و هدف آنها، به‌دست آوردن اطلاعات مهم و حساس دشمن برای کسب برتری استراتژیک است. یکی از مشخصات قابل تأمل در این نوع جنگ‌ها، کاهش هزینه‌ها و تلفات نیروی انسانی با استفاده از دانش برتری در جبهه‌های نبرد است و از سوی دیگر نیز باعث بروز نوعی توازن بین طرفین جنگ می‌شود. به این مفهوم که طرفین درگیر با در اختیار داشتن اطلاعات کافی از دشمن، نقاط ضعف و قوت خود را شناسایی کرده و از عنصر دانایی برای ایجاد برابری با طرف مقابل بهره‌گیری می‌کنند. از دیگر تحولات ناشی از جنگ‌های مجازی در سازوکار نظامی کشورها، سوق دادن آنها به سمت ساختار شبکه‌ای و غیرمتمرکز است. «Network and Decentralization System» مستلزم مهندسی مجدد شیوه‌های کنترل و فرماندهی ارتش‌ها است و در آن ترکیب دو پارامتر مهم عدم تمرکز و کسب دانش برتر، تعیین‌کننده میزان برتری و امتیازات نظامی نیروهای مسلح یک کشور است. به بیان دیگر، جنگ مجازی «Cyber War» با ایجاد تحول در نحوه سازماندهی، استقرار و آموزش نیروهای نظامی و همچنین تصمیم‌گیری در مورد استفاده از انواع کامپیوترها و حسگرهای مورد نیاز در یک عملیات جنگی، شیوه‌های جنگی سنتی را تاریخ مصرف گذشته و ناکارآمد عنوان کرده و استراتژی و تاکتیک‌های مورد استفاده در میادین نبرد را با تغییرات بنیادین، مواجه با خطر خواهد کرد.

در حال حاضر نیز، هم آمریکا و متحدانش و هم دشمنان آنها در حیطه جنگ‌های کم‌شدت در باب تروریسم، قاچاق موادمخدر، سلاح و درگیری‌های نژادی و غیره، از شیوه‌های سازماندهی شبکه‌ای[3] استفاده می‌کنند که به عقیده صاحبنظران مسائل تاکتیکی، حاکی از این

---

1. VOA news
2. Cyber Wars
3. Network Organized

واقعیت است که شبکه‌ها می‌توانند نهادهای متمرکز قدرت را شکست دهند و تنها راهکار منطقی و عملی در جنگ‌های عصر انقلاب اطلاعات، استفاده از شبکه‌های اطلاعاتی است که با ابزارهای مدرن فناوری اطلاعات تجهیز شده‌اند.

«براساس گزارش سایت www.jihadunspan.com ارتش آمریکا با ارسال ایمیل‌هایی به مقامات بلندپایه و ارتش و مردم عراق از آنها خواسته‌اند است تا برای حفظ خود و خانواده‌هایشان از دستورات صدام سرپیچی کنند و اگر اطلاعی در مورد محل اختفای سلاح‌های هسته‌ای، بیولوژیک و شیمیایی دارند با ارسال ایمیل به اطلاع برسانند، در غیر این صورت آمریکا به عراق حمله خواهد کرد. براساس این گزارش، پیام‌های ارسالی از آمریکا به زبان عربی و از سوی پنتاگون صورت گرفته است. صدام نیز در واکنش به این جنگ اطلاعاتی که به‌وسیله دنیای کامپیوتر و اینترنت[1] صورت می‌گیرد، جلوی تمام نامه‌های الکترونیکی ارسالی از آمریکا را گرفته است.»[۴۰]

با توجه به این خبر می‌توان گفت، دسترسی نظامیان و مقامات مختلف به اینترنت در هنگام بحران و جنگ می‌تواند یکی از نقاط آسیب‌پذیر تلقی شود، چرا که امکان مبادله پیام میان اتباع کشور هدف به کشور مهاجم را به راحتی فراهم می‌کند. نباید از یاد برد که در هر حال ایده اولیه اینترنت، توسط وزارت دفاع آمریکا ارائه شده و اکنون به این صورت در اختیار ماست. اینکه چگونه می‌توان مانع ارسال ایمیل شد، امر ساده‌ای ـ آن‌گونه که در انتهای خبر مذکور آمده است ـ نیست و اصولاً جلوگیری از ارسال یا وصول نامه‌هایی از مبدأ یک کشور، فقط یک ادعای گزاف است که توسط غیرمتخصصان ابراز می‌شود. یک ایمیل می‌تواند با هر آدرسی و از هر کشوری ارسال شود و نام و آدرس و IP آن هرگز نشان‌دهنده هویت واقعی ارسال‌کنندگان آن نیست. اینکه چه راه‌حلی برای پیشگیری از این مسئله وجود دارد، مستلزم مباحث عمیق کارشناسی است. حتی اگر مثلاً یک مقام نظامی را از اینترنت در محل کار و منزلش محروم کنیم، درصورتی‌که او یا هر شخص دیگری بخواهد پیام از طریق اینترنت مبادله

1. Computer and Internet World

کند، خواهد توانست در نزدیک‌ترین کافی‌نت موجود در میان صدها کافی‌نت شهر، این کار را انجام دهد مگر اینکه در ایام بحران، کل شبکه اینترنت مسدود شود و یا کار فرهنگی و اطلاعاتی دقیقی بر روی گروه‌های مورد نظر صورت گیرد.

۱۰ـ۱ـ برنامه نظارت بر اینترنت در آمریکا

روزنامه نیویورک تایمز گزارش داد، دولت بوش قصد دارد به ساخت یک سیستم مرکزی ناظر بر اینترنت کمک کند. این مسئله، بخشی از پروژه اصلی اداره امنیت ملی آمریکا می‌باشد که سال ۲۰۰۴ آماده می‌شود. براساس این گزارش، این اداره هدف از ایجاد شبکه‌های کامپیوتری دفاع ملی[1] را نه تنها جلوگیری و از بین بردن ویروس‌های کامپیوتری[2] مخرب، بلکه ممانعت از حملات تروریستی می‌داند. برنامه‌ای در دست تهیه است تا یک استراتژی امنیتی[3] برای اداره جدید امنیت آمریکا طرح‌ریزی شود. پیشنهاد مذکور که به کنگره آمریکا رفته، نیاز به تأیید و تصویب دارد. ایجاد یک اداره مرکزی نظارت و کنترل بر اینترنت و تهیه یک آیین‌نامه کاری برای مراکز خدمات دهنده اینترنتی با وجود هزاران ISP که در میان آنها غول‌هایی همانند مایکروسافت «Microsoft» و ورلد کام[4] به چشم می‌خورند، بسیار مشکل است. به هر حال سیستم مذکور به‌گونه‌ای پایه‌ریزی می‌گردد که با بررسی محتویات برخی سایت‌ها قبل از انجام حملات تروریستی[5] هشدار دهد، بدین مفهوم که اینترنت با توانایی‌هایی که دارد، بتواند نه تنها از خودش بلکه از دیگران نیز در برابر حملات، محافظت نماید.

ایجاد این سیستم با انتقاد شدیدی روبرو گشته است. مخالفان می‌گویند، این طرح شبیه جاسوسی[6] مورد استفاده توسط FBI است، اما سخنگوی دفتر امنیت اظهار داشته است: «هدف ما کنترل صرف اینترنت نیست.»(۴۱)

---

1. Computer Network for National Defence
2. Viruses
3. Security Strategy
4 World.com
5. Terrorist Attack
6. Spying

روز ۲۰ فوریه ۲۰۰۳ روزنامه نیویورک تایمز، پرده از روی یکی از عظیم‌ترین طرح‌های تحریف افکار[1] تاریخ برداشت. پنتاگون در تبعیت از اوامر رامسفلد و داگلاس فیث، معاون وزیر دفاع، به‌منظور احاطه بر «کارزار اطلاعاتی»[2] به‌طور محرمانه، نهادی مرموز به نام دفتر نفوذ استراتژیک «OIS» با هدف نشر اخبار بی‌اساس در خدمت منافع ایالات‌متحده ایجاد کرد و ریاست آنرا به یک ژنرال نیروی هوایی، سیمون وردن، سپرد. این دفتر مجاز بود تا رسماً به شیوه‌های تحریف افکار عمومی[3] به‌ویژه در رابطه با رسانه‌های خارجی متوسل شود. نیویورک تایمز، تصریح کرد که OIS قراردادی بالغ بر ۱۰۰ هزار دلار در ماه با کابینه ارتباط جمعی، راندون گروپ[4] منعقد نموده بود. این کابینه در سال ۱۹۹۰ نیز به هنگام تدارک جنگ خلیج‌فارس به همکاری دعوت شده بود و همین کابینه است که اعلامیه دروغین «پرستار» کویتی که گویی خود شاهد حمله سربازان عراقی به زایشگاه بیمارستان کویت و جدا کردن وحشیانه نوزادان زودرس از تختشان و قتل بی‌رحمانه آنان با پرتابشان به روی زمین بوده، منتشر کرد. این شهادت، تأثیری قاطعانه در جلب آرای اعضای کنگره به نفع جنگ داشت. این دفتر که رسماً پس از افشاگری‌های مطبوعات[5] منحل شد، بی‌تردید همچنان به فعالیت خود ادامه می‌دهد، در غیر اینصورت چگونه می‌توان برخی از زننده‌ترین تحریف‌های اخبار[6] در جنگ اخیر عراق را توجیه نمود.[۴۲]

1. Opinion Distortion
2. Information Operation
3. Public Opinion Distortion
4. Randon Group
5. Press Reveals
6. News Distortions

فصل دوم

۱ـ۲ـ هک کردن و نفوذ به کامپیوترها[1]

در این قسمت به بررسی موارد نفوذ به کامپیوترها از راه دور، نحوه انجام آنها و کاری که متجاوزان در زمان کسب دسترسی انجام می‌دهند، می‌پردازیم. این اقدامات، همانند کلاهبرداری‌های[2] تحمیلی محسوب می‌شوند، چراکه کاربرد کامپیوتر بر دیگر حساب‌ها تحمیل می‌گردد. متجاوزان با خرج و هزینه شخص دیگری نوعی سواری رایگان به‌دست می‌آورند. حتی اگر فعالیت آنان باعث به‌وجود آمدن هزینه‌های واقعی نشود برای صاحبان سیستم که زمانی را صرف ردیابی فعالیت آنها و پاکسازی شلوغی دیجیتالی[3] که خود بر جای گذاشته‌اند می‌نمایند، هزینه‌هایی تحمیل می‌کند. خسارت‌ها می‌توانند قابل ملاحظه باشند، به‌خصوص اگر داده‌ها حذف شوند و قابل بازیابی نباشند.

همچنین این بخش به بررسی حملاتی می‌پردازد که با حملات موسوم به «قطع سرویس»[4] از راه دور، سیستم‌ها را فلج می‌کند، حتی لازم نیست مهاجمان وارد کامپیوترهایی شوند که می‌خواهند آنرا از کار بیندازند.

علاوه بر این، نمونه‌هایی از ابزارها و تکنیک‌های هک کردن ارائه می‌شود، اما این موارد جامع و کامل نیستند. یکی از منابع راهنمای خوب و عمقی برای هک کردن، کتابی به نام The

---

1. Hacking and Influence to Computers
2. Fraud
3. Digital Confusion
4. Denial of Services

Happy Hacker نوشته کارولین مانیل[1] است. در ایران هم کتاب‌های متعددی در زمینه هک‌کردن منتشر گشته و حتی آموزش هک به علاقه‌مندان داده می‌شود!

۲ـ۲ـ هک چیست و هکر کیست؟

Hack به زبان ساده و شاید عامیانه‌ترین تعبیر آن دزدیده شدن کلمه عبور یک سیستم و یا account می‌باشد. به‌طور کلی نفوذ به هر سیستم امنیتی کامپیوتری را hack می‌گویند.

Hacker شخصی باهوش، فرصت‌طلب، دارای معلومات بالا با افکار سازنده و مطمئناً با وجدان است.

لازم به ذکر است که هکرها با دزدان اینترنتی و یا الکترونیکی تفاوت دارند. هکرهای واقعی در میان خود دارای مرام‌نامه‌ای هستند که همه پایبند به آن می‌باشند.

هکر در موقع هک کردن یک سیستم امنیتی، هدفش ضربه زدن (چه مادی و چه معنوی) به شخص و یا اشخاصی نمی‌باشد. او هک می‌کند تا معلوماتش را نشان دهد. هک می‌کند تا همگان بدانند که سیستم‌های امنیتی دارای مشکل هستند. هک می‌کنند تا نواقص (سوراخ‌های)[2] این سیستم‌ها نمایان شوند. اگر هکرها نبودند مطمئناً سیستم‌های امنیتی به کاملی سیستم‌های امروزی نبود، پس هکرها مفیدند.

در این میان، افرادی هستند که با سوءاستفاده از معلومات خود و یا دیگران، هدفشان از هک کردن، ضربه زدن به اشخاص است و یا به‌دنبال پرکردن جیب خود می‌باشند، اینها دزدانی بیش نیستند.

۳ـ۲ـ چگونه هک می‌شویم؟!

از هکری پرسیدند رایج‌ترین و مطمئن‌ترین روش هک کردن چیست؟ او در جواب گفت:

---

1. Carolin Manil
2. Bags

رایج‌ترین روش، ساده‌ترین روش است. یکی از متداول‌ترین روش‌های هک کردن، حدس زدن password است.

روش رایج دیگر خواندن password از روی دست User به هنگام تایپ آن می‌باشد و یا فرستادن صفحه‌ای مانند صفحه ورودی Hotmail, Yahoo به‌صورت یک Email که در آن به ظاهر کارکنان شرکت سرویس‌دهنده از user خواسته‌اند. به‌منظور اطمینان از صحت سرویس‌دهی password خود را تایپ کنید که این password در همان لحظه برای هکر mail می‌شود.

برنامه جالبی وجود دارد که LOG تمامی حروف‌هایی که وارد شده است را ذخیره می‌کند. هکر، برنامه را اجرا می‌کند و بعد از شما می‌خواهد که رمز خود را بزنید. کلیدهای تایپ شده توسط شما درون یک فایل متنی TXT ذخیره می‌شود و هکر بعداً به آن رجوع می‌کند و رمز شما را کشف می‌نماید.

روش دیگر حدس زدن جواب سؤالی است که شما انتخاب نموده‌اید تا در صورت فراموش نمودن رمزتان از شما پرسیده شود. در yahoo استفاده از این روش مشکل است، زیرا تاریخ دقیق تولد، آدرس و حتی کدپستی را نیز می‌خواهد. اما در سرویس hotmail به سادگی می‌توانید جواب سؤال را حدس بزنید و رمز را به‌دست آورید و هکر نیز می‌تواند به کارکنان hotmail نامه زده و در آن ابراز کند که account او مورد هک قرار گرفته و درخواست رمز جدیدی کند که کارکنان Hotmail از او چند سؤال در مورد سن و آخرین دسترسی به account و آخرین رمزی که به خاطر دارد، می‌کنند و سپس رمز جدید در اختیار او قرار می‌گیرد یا برای یافتن رمز accountهای اینترنت، به ISP شما زنگ می‌زند و با دادن مشخصات، خواستار تغییر رمز می‌شود. جالب اینجاست که در بسیاری از موارد منشیان رمز قبلی را نمی‌پرسند.

اینها همه روش‌هایی ساده اما رایج و متداول بودند. روش دیگر کمی تخصصی است و هر شخصی نمی‌تواند از این روش استفاده کند، چراکه باید معلوماتی در خصوص اینترنت و IP و یک سری نرم‌افزارها داشته باشد.

در این روش، شخص با فرستادن یک فایل آلوده بـه ویـروس یـا Trojan سیـستم شـما را آلوده می‌کند. با اجرای این فایل، فایل مورد نظـر در حافظـه جـای مـی‌گیـرد و هـر زمـان کـه کامپیوتر روشن شود دوباره در حافظه ثبت می‌شود. پس با پاک نمودن فایل اولیه، مشکل شـما حل نمی‌گردد. این فایل، کامپیوتر شما را به عنوان یک Server درمی‌آورد و یکی از پرت‌هـا را برای استفاده هکر باز می‌گذارد. (برخی از این Trojanها پرتی را باز نمی‌گذارند بلکه از طریق email رمزها را برای هکر ارسال می‌نمایند). حال هکر می‌تواند با پیدا کردن IP شما و اتـصال به پرت مورد نظر در زمانی‌که هم شما Online هستید و هر کاری با کامپیوتر شما بکنـد، آنـرا گوش کند و در نتیجه رمزهای موجود در کامپیوتر شما را بدزدد.

البته ارسال فایل گاهی به‌صورت Online نمی‌باشد. هکر می‌تواند اگر با شما آشنایی داشـته باشد به پشت کامپیوتر شما بیاید و فایل مورد نظر را روی آن اجرا کند. جالـب اینجاسـت کـه اغلب ویروس‌کش‌ها از شناسایی Trojanهای جدید عاجزند.

۴ـ۲ـ چگونه هک نشویم؟!

روش‌های ساده را به سادگی و با کمی دقت می‌توان مسدود کرد. مثلاً رمزی انتخاب کنیـد کـه حدس‌زدنش کار هر کسی نباشد. شماره تلفن، اسم، فامیل، شماره شناسنامه یـا تـاریخ تولیـد و ترکیبی از اینها معمولاً اولین چیزی است که به ذهن هر کـسی مـی‌رسـد. سـعی کنیـد در رمـز انتخابی خود از پرانتز یا کروشه استفاده کنید و یا حتی کامـا کـه اینهـا بـه ذهـن هـیچ هکـری نخواهد رسید. هنگامی که رمز خود را وارد می‌کنید مراقب باشید، شخصی نزدیکتـان نباشـد و یا از کلیدهای منحرف‌کننده استفاده کنید. مثلاً چند کلید را الکی بزنیـد و بعـد بـا Backspace پاکش کنید که اگر کسی هم دید، متوجه رمز شما نشود.

پشت کامپیوتر فردی که به او اطمینانی نداریـد، رمـزی وارد نکنیـد، یـا اگـر مجبوریـد، بـا استفاده از کلیدهای Ctrl+Alt+Del و باز نمودن Task Manager کلیه برنامه‌های مـشکوک را ببندید. معمولاً اسامی آنها مانند Thief، Keylogger یا Key و یا هـر اسـم مـشکوک دیگـری

می‌تواند باشد. در زمان ثبت‌نام در سرویس‌های Hotmail و Yahoo به شما تذکر داده می‌شود که کارکنان شرکت سرویس‌دهنده به هیچ عنوان از طریق Email از شما درخواست Password نمی‌کنند. پس هرگز از طریق هیچ ایمیلی رمز خود را وارد نکنید. از مکانی اینترنت را تهیه کنید که امنیت بیشتری دارد و تجربه کارشان بالاست، زیرا علاوه بر منشیان بی‌تجربه که بعضاً رمزها را بر باد می‌دهند، اگر شبکه (ISP) هک شده باشد، دیگر از دست شما کاری بر نمی‌آید و رمز شما و دیگر کاربران در خطر می‌باشد.

احتمال حمله با روش تخصصی فوق به کاربرانی که از سیستم‌های Instant messaging مانند Yahoo messenger و یا MSN messenger و یا ICQ و ... استفاده می‌کنند، بیشتر است، چون این‌گونه برنامه‌ها به راحتی IP شما را در اختیار هکر قرار می‌دهند و همواره یک پرت آزاد را اشغال می‌کنند و معمولاً به‌صورت مستقیم با کاربر مقابل در ارتباط هستند، به‌خصوص در مواقع ارسال و دریافت فایل. پس اگر می‌خواهید در امان باشید از این برنامه‌ها استفاده نکنید.

اما امروزه در ایران، اینترنت بدون این‌گونه برنامه‌ها فایده‌ای ندارد! پس هیچ‌گونه فایلی را که از افراد ناشناس فرستاده می‌شود، باز نکنید. حال اگر کامپیوتر شما از قبل آلوده شده باشد، چه باید کرد؟!

اگر مطمئن‌ترین راه را می‌خواهید، کامپیوتر خود را فرمت نموده و دوباره ویندوز را نصب کنید. زیرا اغلب ویروس‌کش‌ها قادر به شناسایی و یا پاک نمودن بسیاری از این نوع ویروس‌ها نمی‌باشند. اما معمولاً این روش به صرفه نیست. کاری که برای مبارزه با این نوع ویروس‌ها توصیه می‌شود این است که یک ویروس‌کش جدید نصب کرده و هر هفته آنرا Update کنید. Norton Antivirus 2002 پیشنهاد می‌شود که خود به‌صورت اتوماتیک هر ۱۰ روز یک‌بار به روز شود. حال اگر ویروسی پیدا شد که ویروس‌کش نتوانست آنرا شناسایی کند چه؟!

فایلی که در حافظه شما اجرا می‌شود و کامپیوتر شما را به‌عنوان Server آماده حمله هکر می‌کند برای اتصال به اینترنت و فرستادن اطلاعات احتیاج به یک پرت آزاد دارد. روش‌های

بسیاری برای مسدود نمودن پرت‌های آزاد وجود دارد. در ایران همواره مرسوم است که می‌گویند اینترنت بدون Proxy بهتر است، اما باید بدانید که Proxy نه تنها سرعت کار شما در اینترنت را بالا می‌برد بلکه جلوی حمله هکرها را نیز می‌گیرد.

روش دیگر استفاده از Firewall می‌باشد. امروزه بسیاری برنامه‌های کم‌حجم با عنوان Firewall خانگی وجود دارند.

شما با استفاده از یکی از این برنامه‌ها می‌توانید به راحتی هرگونه رد و بدل شدن اطلاعات بین کامپیوتر خود و اینترنت را ببینید و کنترل نمایید. برنامه‌ای که پیشنهاد می‌شود، ZoneAlarm است. با نصب این برنامه هرگاه، برنامه‌ای بخواهد با اینترنت تبادل اطلاعات نماید، ابتدا به شما تذکر می‌دهد و شما می‌توانید اگر برنامه مشکوکی بود اجازه فرستادن اطلاعات را از او سلب کنید. در ضمن، هیچ شخص و برنامه‌ای هم نمی‌تواند بدون اطلاع شما از بیرون به کامپیوتر شما متصل شود. ویندوز XP از نظر امنیت در شبکه بسیار پیشرفته و احتمال هک شدنش کمتر است، پیشنهاد می‌شود از این ویندوز استفاده کنید.

در آخر باید گفت هیچ روشی به‌صورت ۱۰۰٪ شما را ایمن نمی‌سازد، بلکه فقط سعی می‌کنیم احتمال هک‌شدنمان را پایین آوریم.(۴۳)

۵ـ۲ـ هکرهای کلاه سفید و هکرهای کلاه سیاه

هکرها دو دسته‌اند: کلاه سفیدها[1] و کلاه سیاه‌ها[2]. هکرهای کلاه سفید متخصصان و کامپیوتر دوستانی هستند که سعی می‌کنند عیوب امنیتی[3] در یک سیستم کامپیوتری را پیدا کرده و آنها را برطرف سازند. بسیاری از شرکت‌ها، هکرهای کلاه سفید را برای آزمایش شبکه‌های کامپیوتری[4] و خدمات اینترنتی[5] خود استخدام می‌کنند. افزون بر این، بسیاری از سازندگان برنامه‌های کاربردی اغلب خودشان، برنامه‌های خودشان را هک می‌کنند تا آسیب‌پذیری‌های

1. White hats
2. Black hats
3. Security Faults
4. Computer Networks
5. Internet Services

آنها را بیابند. در واقع کلاه سفیدها برای اینکه کار خود را انجام دهند، مجبورند همچون کلاه سیاه‌ها عمل کنند تا بتوانند حفره‌های امنیتی سیستم‌ها[1] را بیابند. برخی از هکرهای کلاه سفید بازی دوستان و کاربرانی هستند که در اوقات فراغت خود به آزمایش بر روی برنامه‌هایی که به‌کار می‌برند، می‌پردازند و نتیجه آزمایش خود را به صورت رایگان برای سازندگان آن برنامه ارسال می‌کنند.

اهداف کلاه سفیدها، کاملاً اخلاقی است. کلاه هکرهای کلاه سفید، همین که بدون اجازهٔ صاحب یک سیستم به آن سیستم نفوذ می‌کنند ـ که از لحاظ فنی جرم است ـ رنگ عوض کرده و تیره به‌نظر می‌رسند. این دسته از هکرها مانند «تام سرونکا» که به سیستم eBay , Hotmail نفوذ کرد و بی‌آنکه به آنها صدمه‌ای وارد کند حفره‌های امنیتی آنها را فاش نمود، به هکرهای کلاه خاکستری شهرت یافته‌اند.

یک هکر کلاه خاکستری[2] دیگر «آریان لامو»[3] نام دارد که تیم‌های یاهو، مایکروسافت و نیویورک را هک کرد و اشکالات و حفره‌های آن سیستم‌ها را به صورت رایگان در اختیار صاحبان آن تیم‌ها قرار داد. برخی از کلاه سفیدها حفره‌هایی را می‌یابند که از طریق تماس مستقیم به مدیران اطلاع می‌دهند و بعضی از آنها یک پیغام در سیستم به جای می‌گذارند و در آن وجود حفره‌ها را به مدیران گزارش می‌دهند.

کلاه خاکستری‌ها تردّیدهایی در مورد خلوص نیت خود به‌وجود می‌آورند، زیرا آنها اغلب با انتشار دادن عیوب امنیتی در رسانه‌ها و اینترنت به‌دنبال شهرت هستند. بعضی از متخصصان استفاده از اصلاحاتی چون «هکر کلاه سفید» را درست نمی‌دانند. آنها معتقدند که وقتی صاحب یک سیستم خودش بخواهد که سیستم وی مورد هک واقع شود، این عمل هک نیست بلکه یک سرویس است. آنها عمل هک را یک فعالیت غیرقانونی می‌دانند.

با آنکه کلاه هکرهای کلاه سفید می‌توانند گاهی به کلاه خاکستری تبدیل شوند، اما کلاه

---

1. Security Bags in System
2. Grey hat
3. Arian Lamo

هکرهای کلاه سیاه واقعاً سیاه هستند، چون آنها سوءنیت دارند. هکر کلاه سیاه به فردی اطلاق می‌شود که به‌منظور صدمه زدن وارد یک سیستم می‌شود. هکرهای کلاه سیاه به روش‌های مختلفی کار می‌کنند. در سال‌های اخیر آنها به پایگاه‌های مشهوری چون Amazon , eBay , Msubc ضربه وارد کرده و حتی آنها را خارج از سرویس نموده‌اند. این حملات معمولاً با استفاده از کامپیوترهای به دام افتاده دیگران صورت گرفته است. بهترین عمل هکر کلاه سیاه، شامل دزدی و اخاذی می‌شود.

در سال ۱۹۹۴، یک باند هکر[1] در مسکو به شبکه Citibank نفوذ کردند و ۱۰ میلیون دلار را به حساب خود انتقال دادند. سایر هک‌های مجرمانه، شامل دریافت شماره کارت‌های اعتباری مشتریان یک شرکت اینترنتی است. هکرهای کلاه سیاه معمولاً اطلاعات خود را درباره حفره‌های امنیتی از طریق اینترنت به سایر هکرهای کلاه سیاه در سراسر دنیا انتقال می‌دهند. آیا هکرهای کلاه سیاه هم در جامعه طرفدارانی دارند؟ بعضی از مردم یک گروه از هکرهای کلاه سیاه را که روزبه‌روز هم بیشتر می‌شوند، تحسین می‌کنند؛ هکرهایی که پایگاه‌های پورنوگرافیک را هدف قرار می‌دهند و به آنها ضربه می‌زنند.

گروه جدیدی از هکرهای جوان، مشهور به بچه‌های اسکریپتی، Kiddies Script نیز ظاهر شده‌اند که با هکرهای کلاه سیاه تفاوت دارند. هکرهای کلاه سیاه به اینکه خودشان برنامه می‌نویسند و حفره‌های امنیتی را از طریق معلومات خود می‌یابند، می‌بالند. بچه‌های اسکریپتی با استفاده از برنامه‌های خدماتی ویژه هک که به‌وسیله دیگران نوشته شده و از طریق اینترنت می‌توان آنها را دریافت کرد به پایگاه‌های وب خسارت وارد می‌کنند. این برنامه‌ها به‌دنبال درگاه‌های باز بر روی شبکه‌های مبتنی بر وب می‌گردند یا به شبکه یک کتابخانه یا مدرسه نفوذ می‌کنند تا حملات خارج از سرویس‌سازی Attack Denial of Service را تدارک ببینند. بسیاری از متخصصان معتقدند که ظهور رو به گسترش بچه اسکریپتی‌ها جدی‌ترین تهدید را برای امنیت کامپیوتر به‌وجود آورده است، چرا که از کار انداختن یک پایگاه وب و یا نفوذ به

1. Hacker Clique

یک شبکه دیگر به دانش کامپیوتری پیشرفته نیاز ندارد و بچه‌های اسکریپتی در ایران نیز با سرعت بسیار بالایی در حال افزایش می‌باشند.

هکرهای کلاه سیاه و کلاه سفید اغلب به مکان‌های مشابه نگاه می‌کنند و از ابزار مشابه برای یافتن حفره‌های امنیتی بهره می‌گیرند. اختلاف اصلی در نحوه پاسخ هر گروه هکری به موقعیت، مشابه است. در بخش زیر چندین مثال در این رابطه آمده است:

۱. وضعیت استفاده از یک برنامه پی برنده بسته که یک نوع برنامه خدماتی است که می‌تواند تمام بسته‌بندی‌های اطلاعاتی در حال نقل‌وانتقال بر روی شبکه را بخواند؛

۲. یافتن حفره‌ای[1] در یک پایگاه تجارت الکترونیکی[2] که اطلاعات کارت اعتباری مشتریان یک شرکت را فاش می‌کند؛

۳. یافتن روشی برای تغییر دادن محتویات یک پایگاه وب[3]؛

۴. کشف یک ویروس[4] یا یک کرم[5]؛

۵. نفوذ به یک PC خانگی از طریق مودم؛

کلاه سفید

۱. از آن به‌عنوان وسیله تشخیص عیب در شبکه‌ها یا حتی تشخیص نفوذ هکرها بهره می‌گیرد. نقطه آسیب‌پذیر را به شرکت اطلاع می‌دهد و یا در حالت یک هکر کلاه خاکستری، ضعف‌های امنیتی را در اختیار مطبوعات می‌گذارد.

۲. به مدیر سیستم[6] مسئله را اطلاع می‌دهد، یا یک پیغام بی‌ضرر[7] در شبکه می‌گذارد تا مدیران شبکه نقطه آسیب‌پذیر را بشناسند.

۳. آنرا به مرکز Cert که یک سازمان پاکسازی ویروس است، اطلاع می‌دهد.

---

1. Bag
2. E-Commerce Website
3. Website
4. Virus
5. Worm
6. Manager System
7. Harmless Message

۴. نقطه آسیب‌پذیر را به ISP اطلاع می‌دهد.

۵. از آن هیچ‌گونه استفاده‌ای نمی‌کند.

کلاه سیاه

۱. کلاه سیاه از آن برای خواندن داده‌های حساس و در حال نقل‌وانتقال یک شبکه، به‌ویژه کلمه‌های عبور بهره می‌گیرد.

۲. بعدها او می‌تواند با کلمه عبور کشف شده، اطلاعات مهم و محرمانه را به‌دست آورد.

۳. چهره پایگاه وب مزبور را عوض می‌کند، یا محتویات آنرا تغییر می‌دهد.

۴. سعی می‌کند شبکه یک شرکت خاص را معمولاً بدون دلیل انتقام‌گیری، آلوده کند.

۵. PC کاربر را جست‌وجو می‌کند تا کلمه‌های عبور[1] یا اطلاعات کارت اعتباری او را بیابد.

هک، دنیای پیچیده‌ای است، اما فرهنگ هک[2] تقسیم‌بندی ساده‌ای برای انواع هکرها دارد: هکرهای کلاه سفید[3] و هکرهای کلاه سیاه[4]. هکرهای کلاه سفید به افرادی گفته می‌شود که به پیشرفت امنیت در دنیای دیجیتال فکر می‌کنند و هکرهای کلاه سیاه افرادی هستند که امیدوارند از ضعف‌های سیستم‌های دیگران به نفع خود بهره برند. این اصطلاحات از سینمای وسترن گرفته شده که در آنها آدم‌های خوب، کلاه سفید و آدم‌های بد، کلاه سیاه بودند.[۴۴]

۶ـ۲ـ حساب‌ها[5]

فرآیند نفوذ در کامپیوتر معمولاً شامل دسترسی به حساب موجود در سیستم است. فرد متجاوز با اتصال به این حساب می‌تواند هر اقدامی را که برای آن حساب به‌خصوص مجاز است، انجام دهد مانند دسترسی به فایل‌ها[6]، اجرای برنامه‌های کامپیوتری برای خواندن و دستکاری

---

1. Passwords
2. Hack Culture
3. White hat hacker
4. Black hat hacker
5. Accounts
6. Access to Files

اسناد، خواندن پیام‌های پست الکترونیک (E-mail) که به آن حساب فرستاده شده‌اند، ارسال پیام‌های الکترونیکی[1] از آن پیام و انهدام فایل‌ها[2].(۴۵)

خلاصه اینکه فرد متجاوز دسترسی بی‌حد و حصری به حساب پیدا می‌کند و با آن می‌تواند به تمام منابعی که در دسترس آن حساب است، نفوذ کند.

خسارتی که به بار می‌آید، بستگی به اقداماتی دارد که با حساب به مخاطره افتاده عملی می‌شوند. مثلاً شرکت America Online دارای انواع مختلفی از حساب‌ها می‌باشد. حساب‌های مشتریان معمولاً به‌طور کامل محدود بوده و فقط دسترسی به اطلاعات عمومی و پیام الکترونیکی آن عضو را که برای هر یک از کاربران AOL در دسترس هستند، فراهم می‌کند. حساب‌های بالاسری (over head) که استفاده نامحدود را بدون هیچ هزینه‌ای امکان‌پذیر می‌سازند، مورد استفاده ارائه‌دهندگان این حساب‌ها قرار می‌گیرند تا مطالبی را بر روی سیستم قرار دهند. هکری که به یکی از این موارد دسترسی پیدا می‌کند، می‌تواند در مناطقی که کاربران AOL می‌بیند، خرابکاری کند.(۴۶)

بسیاری از سیستم‌ها دارای حساب ویژه‌ای به نام حساب «ریشه‌ای» (root accunt) بر روی سیستم‌های یونیکس و حساب «مدیر» (Administor) در ویندوز N.T[3] هستند. این حساب، مورد استفاده مدیران سیستم می‌باشد تا سیستم را اداره کنند. هرکس که به این حساب وصل شود به تمام برنامه‌ها و داده‌های موجود بر روی سیستم، دسترسی پیدا می‌کند. از این حساب، فرد متجاوز می‌تواند هر برنامه‌ای را اجرا کند و هر فایلی را خوانده، تغییر داده یا حذف کند. وقتی حساب یک کاربر به خطر می‌افتد، در اغلب موارد دسترسی به حساب ویژه آسان می‌شود.

هکرها در اغلب موارد حساب‌های خود را بر روی دستگاه‌هایی که به آنها نفوذ دارند، یا دسترسی می‌یابند ایجاد می‌کنند.(۴۷)

---

1. Electronic Messages
2. Destruction of Files
3. Windows N.T

دسترسی پیدا کردن[1]

فرد متجاوز برای دسترسی داشتن به یک حساب، ابتدا باید به دستگاهی که میزبان (host) آن حساب است، دسترسی داشته باشد، چه از طریق یک خط dial-in و چه از طریق یک ارتباط شبکه‌ای. اگر سیستم بر روی اینترنت است و فرد متجاوز نام قلمرو (domain name) یا آدرس IP آنرا بداند، در این صورت یکی از راه‌های متصل شدن از طریق TELNET است که خود جزو برنامه‌های کاربردی اینترنت برای اتصال از راه دور محسوب می‌شود.(۴۸)

برای نشان دادن این مفهوم فرض کنید، متجاوزی می‌خواهد به یک کامپیوتر فرضی در آدرس cool.victim.com دسترسی پیدا کند. او برنامه TELNET را فعال کرده و هنگامی که از او نام قلمرو پرسیده می‌شود، تایپ می‌کند: cool.victim.com یا اینکه یک پارامت فرمان تایپ می‌کند: Telnetcool.victim.com. پس از اینکه اتصال برقرار شد، دستگاهی که در دوردست قرار دارد نام حساب (account name) و اسم رمز را درخواست می‌کند. اگر متجاوز با یک شماره معتبر[2] پاسخ دهد، آن دستگاه یک پارامت فرمان برخواهد گرداند. در این مرحله متجاوز می‌تواند دستورهایی به آن دستگاه بدهد، مثلاً "dir" یا "LS" تا فهرستی از تمام فایل‌های موجود در دایرکتوری آن حساب به‌دست آورد. وقتی اسامی فایل‌ها مشخص شد، متجاوز می‌تواند فرمان‌های بیشتری برای دسترسی یا حذف فایل‌ها صادر کند: مثلاً "del" برای حذف کردن تمام فایل‌ها در آن دایرکتوری. فرمان‌ها را می‌توان برای راه‌اندازی حمله‌ای به یک کامپیوتر دیگر صادر کرد.(۴۹)

اگر نام حساب و اسم رمز معتبر شناخته نشده باشد، هکر می‌تواند، حدس بزند. بسیاری از کاربرها اسم رمزهای آسانی را انتخاب می‌کنند، مانند نام کاربری یا اسم کوچک خود.(۵۰)

بسیاری از سیستم‌ها با یک اسم رمز و حساب از پیش‌گزیده وارد بازار می‌شوند و

---

1. Access   2. Authoritative Number

هیچ‌گاه تغییر نمی‌کنند. مثلاً یک حساب با نام Guest (مهمان) و اسم رمز guest. هکر می‌تواند در هنگامی که تلاش می‌کند تا وارد کامپیوتر شود این حساب‌ها را امتحان کند.(۵۱)

ابزارها و تاکتیک‌ها[1]

هکرها می‌توانند از انواع وسایل نرم‌افزاری[2] برای کمک گرفتن در حملات خود استفاده نمایند. این وسایل شامل موارد زیر هستند: فرمان‌هایی[3] که بر روی صفحه کلید صادر شده‌اند، برنامه‌ها و اسکریپت‌هایی که توالی فرمان‌های وارد شده به درون یک فایل و اجرا شده به‌صورت یک واحد هستند، عوامل خودمختار[4] که بدون دخالت صاحبان خود اجرا شده و گسترش می‌یابند (مانند کرم‌ها و ویروس‌ها) و جعبه ابزارها (tollkit) که بسته‌های نرم‌افزاری هستند. به مرور زمان، هکرها به‌طور فزاینده‌ای حالت خودکار پیدا کرده و قدرتمندتر می‌شوند و به متجاوزانی که نسبتاً بی‌تجربه هستند، امکان می‌دهند تا به سیستم نفوذ کنند. ابزارهای هک کردن خودکار در اینترنت و از سایت‌های متعدد وب و FTP (پروتکل انتقال فایل) در دسترس همه افراد است.(۵۲)

۷ـ۲ـ اسکنرهای شبکه[5]

کارشناسان امنیت کامپیوتری، ابزارهایی ساخته‌اند تا به مدیران سیستم در امر نظارت بر شبکه‌ها از نظر انواع نقاط ضعف امنیتی موجود کمک کنند. مثال‌های این ابزارها، شامل «اسکنر امنیت اینترنت» (ISS) که کریستوفر کلاوس[6] برنامه‌نویسی کرده و «ابزار تحلیل امنیت برای حسابرسی شبکه‌ها» (SATAN) می‌باشد که دان فارمر[7] و ویسه وینما[8] برنامه‌نویسی کرده‌اند. این برنامه‌ها در اینترنت در دسترس هستند و در آنجا هکرها می‌توانند دیگر اسکنرهای شبکه

---

1. Tools and Tactics
2. Software Equipments
3. Commands
4. autonomous agents
5. Network Scanners
6. Christopher Klaus
7. Dan Farmer
8. Wiets Venema

را بردارند و برای بررسی روزنه‌های امنیتی یک شبکه، درهای باز[1]، اطلاعات عمومی[2] درباره سیستم و بازیابی یک کپی از فایل اسم رمز سیستم را مورد استفاده قرار دهند. این اسکنرها شبیه اسکنرهای پورت[3] هستند، اما اطلاعات بیشتری فراهم می‌کنند. بعضی از آنها دارای رابط کاربری گرافیکی[4] هستند، از اینرو برای اجرای آنها فقط تخصص فنی متوسطی لازم است.(۵۳)

هکرها معمولاً از اسکنرها برای یافتن و بهره‌برداری از نقاط ضعف موجود در سیستم‌ها استفاده می‌کنند.(۵۴)

۸ـ۲ـ Packet Sniffers

شرکت CERT/CC که کار خود را در پاییز سال ۹۳ شروع کرده بود، دسته‌ای از حملات اینترنتی را کشف کرد که اصولاً متفاوت از حملات اولیه بودند. برای به‌دست آوردن اسم رمز و نام کاربری[5] افراد هکرها، مشغول نفوذ به سیستم‌ها و نصب Packet Snifferهایی بودند. استخراج اطلاعات[6] کار دشواری نبود زیرا بسته‌های برقراری ارتباط (login packets) برچسب[7] خورده بودند. در مواردی هکرها وارد سیستم‌های متعلق به شرکت‌های ارائه‌دهنده خدمات اینترنتی می‌شدند که در آنجا حجم عظیمی از داده‌های login را با کمک snifferهای نصب شده خود به‌دست می‌آوردند. یکی از ارائه‌دهندگان منطقه‌ای، پیدا کردن یک 600K Logfile را گزارش کرد که حاوی بیش از ۲۰ هزار اسم رمز و نام کاربری سرقتی بود. حساب‌های به سرقت رفته در آن زمان برای نفوذ در سیستم‌های بیشتر و نصب snifferهای فرعی مورد استفاده قرار می‌گرفتند.(۵۵)

هکرها تلاش بسیاری می‌کردند تا فعالیت خود را مخفی نگاه دارند. آنها برنامه و لاگ‌فایل‌ها را در دایرکتوری‌های بعیدی مانند "tmp/" مخفی می‌کردند و به آنها اسامی

---

1. Open Doors
2 General Information
3. Port Scanners
4. Graphical User Interfaces
5. User Name
6. Extracting the Information
7. Label

مضحکی می‌دادند که با « . »[1] شروع می‌شد. در چند مورد، هکرها سیستم عامل را دستکاری کردند، به طوری‌که ناظر سیستم متوجه اجرای Sniffer نشود، از رمزگذاری نیز استفاده می‌شد تا مدارک مربوط به این حملات مخفی شوند. تا اوایل سال ۱۹۹۵، شرکت CERT/CC تخمین می‌زند که حملات این چنینی برای متجاوزان این امکان را فراهم آورده تا به بیش از صد هزار کامپیوتر در آمریکا و به‌علاوه سیستم‌هایی در آلمان، هلند و سوند نیز دسترسی داشته باشند. بعضی از این حملات مخرب بوده و باعث از کار افتادن شبکه‌ها و دستگاه‌های میزبان می‌شدند. در یک مورد، هکرها هر هارد دیسک موجود در یک شبکه متشکل از ۱۰ دستگاه را از نو فرمت کرده بودند. در پایان سال ۱۹۹۶ این شرکت گزارش داد که packet snifferها همچنان مشکل حادی هستند. این snifferها مکرراً به‌عنوان بخشی از یک ابزار در دسترس نصب می‌شدند که شامل دستورالعمل‌های «آشپزی» بودند که حتی یک تازه‌کار هم می‌توانست از آن پیروی کند.(۵۶)

دو نفر از هکرهای انگلستان به نام‌های مستعار Kuji و Data Stream که در «مرکز توسعه هوایی رم» به سیستم‌ها نفوذ کرده بودند، هفت برنامه Sniffer را که ۳۰ مورد از سیستم‌های رم و بیش از ۱۰۰ نام کاربری و اسم رمز دیگر را به خطر انداخته بودند، نصب کردند. این متجاوزان از حساب‌های به خطر افتاده برای خواندن، کپی کردن و حذف پیام‌های الکترونیکی و همچنین برای خواندن و کپی کردن داده‌های حساس و طبقه‌بندی نشده برنامه شبیه‌سازی میدان جنگ استفاده می‌کردند. وقتی متجاوزان تهاجم خود به سیستم‌های دیگر را توسعه دادند، اقدام به نصب snifferهای دیگری کردند تا به داده‌های بیشتری دسترسی داشته باشند. آنها همچنین یک حمله اسکنری به سیستم‌های متعدد متعلق به یک مقاطعه‌کار هوا ـ فضا به نام آزمایشگاه ملی بروکهیون در نیویورک و در پایگاه نیروی هوایی پاترسون در اوهایو انجام دادند.(۵۷)

از ۱۳۱ حادثه گزارش شده به «مرکز فدرال واکنش به حوادث کامپیوتری» بین نوامبر سال

1. Dot

۱۹۹۶ و ماه مه ۱۹۹۷، حداقل ۱۰ مورد شامل نصب Packet Snifferها بودند. در یک مورد، فرد متجاوز دسترسی ریشه‌ای به یکی از سیستم‌های دولتی به‌دست آورده بود. این Sniffer اطلاعاتی را به مدت ۶ ماه به‌دست آورد و سپس کشف شد. این حادثه، شامل ۳۸۵ سایت و ۵۳۵ کامپیوتر میزبان بود.(۵۸)

۹ـ۲ـ ارتش هکرها

برپایی یک ارتش سنتی کم‌هزینه نیست. یک جنگنده بیش از ۱۰۰ میلیون دلار قیمت دارد، علاوه بر آن باید هزینه ناوها، تانک‌ها، ماهواره‌های جاسوسی و افراد مسلح را نیز در نظر گرفت. در مقایسه با این ارقام هنگفت، تشکیل یک «گروه هکرها» "Hackers Team" مبلغی بین یک تا ۱۰ میلیون دلار هزینه دارد که برای به خدمت گرفتن ۱۰ تا ۲۰ هکر حرفه‌ای جهت راه‌اندازی یک جنگ اطلاعاتی کافی است. این تیم حرفه‌ای را می‌توان با همین مبلغ ۱۰ میلیون دلار به آخرین مدل‌های رایانه نیز مجهز ساخت. ابزارهای هک کردن (Hacking) را نیز بدون هزینه بسیار می‌توان در سراسر سایت‌های اینترنتی جهان به‌دست آورد.

جنگ اطلاعاتی یا استفاده از هکرها، یک جنگ کم‌هزینه، تمیز و بهداشتی و در عین حال مفید و مؤثر است.

۱۰ـ۲ـ نبرد هکرها در جنگ آمریکا ـ عراق

جنگ آمریکا ـ عراق باعث آشکار شدن دوباره جنگ سایبر[1] در عرصه اینترنت شد. اما نه جنگ علیه سایت‌ها و سرورهای عراقی (که تنها چندین سایت و ایمیل آنها از مدت‌ها قبل از کار افتاده بود) بلکه نزاع میان هکرهای طرفدار و مخالف جنگ بود که بیش از همه خود را نشان داد. براساس آمار منتشر شده از سوی شرکت MI2g تنها در روز ساقط شدن مجسمه

---

1. Cyber Warfare

صدام، سه هزار حمله دیجیتالی[1] موفقیت‌آمیز علیه سایت‌های بزرگ آمریکا و انگلیس به ثبت رسید. سایت کوی‌کولا در سنگاپور، فوجی فیلم در آمریکا و سوئیس و حملات ناموفق به ناسداک و بازار بورس آمریکا از جمله آنها بود.

آژانس برآوردهای نظامی انگلیس و بسیاری از سایت‌های حکومتی دیگر انگلیس نیز از این حملات درامان نماندند، البته قبل از آن روز نیز در طول جنگ چندین بار به سایت نخست‌وزیری بریتانیا (تونی بلر) نیز حمله شد. «هکر وایزر»[2] این‌بار به سود آمریکا کنار آمد، اما گروه «ارواح شیطانی»[3] که برزیلی هستند تنها در یک روز، هزار سایت را علیه آمریکائیان هک کردند. Jack-Away یکی از نیروهای «هکر وایزر» گفت: «در جنگ سایبر میان آمریکا و چین ما از خودمان دفاع کردیم». اما گروه "Arabvieruz" که به گفته MI2g از سوی مجامع دانشگاهی عربستان تقویت می‌شود و گروه Dum که از طرف هکرهای اهل مالزی به مخالفان جنگ پیوسته‌اند، رسماً سایت‌های آمریکایی، انگلیسی و طرفداران جنگ را خنثی کردند. از طرف دیگر، نیز سرورها[4] و سایت‌های ایرانی، ترک، امارات، کویت و عربستان نیز مورد حملات Dos قرار گرفته و اختلالات بعضاً شدیدی را در ترافیک شبکه‌های خود پیدا کردند. به هر حال این موج از حملات، نتایج عمده‌ای را به بار آورد. بدبین شدن به اخبار تلویزیون‌های جهان از سوی مخاطبان دنیا و هجوم کاربران به استفاده از اینترنت برای یافتن اخبار صحیح نیز به‌طور غیرمستقیم باعث شد تا هکرها در جنگ سایبر مشارکت فعالانه‌تری داشته و ادعاها و نظرات سیاسی و اخلاقی خود را بروز دهند. از طرف دیگر، این جنگ نشان داد که برای حملات دیجیتالی باید سرورها و سایت‌های خود را آماده پیامدهای ناشی از بحران کرد تا آسیب‌های کمتری به آنها وارد آید.(۵۹)

---

1. Digital Attack
2. Wizer Hacker
3. Satanic Spirits
4. Servers

۱۱ـ۲ـ حملات اینترنتی متقابل[1]

اخلال یا خرابکاری در سایت‌های اینترنتی طرف‌های درگیر جنگ توسط دولت‌ها یا گروه‌های هوادار هر یک از دو طرف درگیر در جنگ، یکی از شیوه‌های متداول جنگ‌های عصر انقلاب اطلاعات است. در طول جنگ آمریکا و انگلیس علیه عراق، ۲۰ هزار سایت اینترنتی مورد حمله هکرها قرار گرفت و در نتیجه از کار افتادند. به گزارش مؤسسه «اف ـ سکیور»[2] که در زمینه «امنیت شبکه‌ها»[3] فعالیت می‌کند تنها در طول یک هفته اول جنگ آمریکا علیه عراق، بیش از ۱۰۰۰ سایت اینترنتی هک شد. بسیاری از این حمله‌ها با نوشتن شعارهای ضدجنگ یا ضدآمریکایی و یا حتی ضدعراقی بر روی وب‌سایت‌ها صورت گرفت. از جمله سایت‌هایی که در این مدت هدف حمله هکرها قرار گرفت، سایت نیروی دریایی و مرکز ملی تحقیقات بهره‌برداری کشاورزی آمریکا بود. گزارش مؤسسه اف ـ سکیور، سه گروه از هکرها را مسئول احتمالی این حملات معرفی کرده است که عبارتند از:

۱. گروهی از میهن‌پرستان در آمریکا؛
۲. گروه‌های تندرو اسلامی؛
۳. فعالان صلح که مخالف جنگ هستند.

کارشناسان معتقدند، هرچند حملات اینترنتی پدیده تازه‌ای نیستند، اما اینکه طرفداران صلح، پیام خود را از این طریق به گوش مردم جهان می‌رسانند، موضوع جالبی است. پیش از شروع جنگ در عراق نیز فعالیت‌های مشابهی از سوی هکرهای اسلام‌گرا مشاهده شده بود. اسرائیل نیز از جمله کشورهایی بود که با افزایش تنش در منطقه، زیر بمباران حملات اینترنتی قرار گرفت. یک کرم رایانه‌ای[4] به نام «گاندا» که از طریق پست الکترونیکی E-Mail منتقل می‌شود، اولین نمونه از ویروس‌هایی بود که با سوءاستفاده از موضوع جنگ و با قول نشان

1. Reciprocal Internet Attacks
2. F-Secure
3. Security of Networks
4. Computer Worm

دادن تصویر ماهواره‌ای[1] از عراق یا برنامه محافظ صفحه[2] از کاریکاتور جورج بوش کاربران را مورد حمله قرار می‌داد.

سایت اینترنتی شبکه تلویزیونی «الجزیره» قطر نیز از جمله سایت‌هایی بود که به‌علت پخش تصاویر کشته‌شدگان انگلیسی و آمریکایی در جنگ عراق، باعث عصبانیت عده‌ای شد و توسط هکرها از کار افتاد. می‌توان چنین احتمال داد که هکرهای به استخدام درآمده پنتاگون، وظیفه انجام چنین عملیاتی را برعهده داشتند، کما اینکه در اقدام کاملاً مشابهی، ارتش آمریکا دفتر شبکه تلویزیونی الجزیره در بغداد را مورد هدف مستقیم راکت قرار داد و طی آن طارق ایوب، خبرنگار شبکه مذکور شد و این دقیقاً مشابه همان رویدادی است که در جنگ افغانستان هم اتفاق افتاد و طی آن دفتر الجزیره در کابُل مستقیماً مورد هدف موشک آمریکایی قرار گرفت. قبل از انجام این عملیات، آمریکایی‌ها در بالاترین سطح، از مقامات قطر خواسته بودند، مانع ادامه روند انتشار اخبار و گزارش‌های جنگی الجزیره شوند، اما قطر زیر بار نرفت و الجزیره به رویه خود ادامه داد.

با جنگ اخیر بحث هک کردن سایت‌ها توسط مخالفان و موافقان جنگ شیوع پیدا کرد و آنها مدام با هک کردن سیستم‌های طرف مقابل پیام‌هایی مانند، یانکی به خانه‌ات برگرد یا خدانگهدار نظامیان و غیره می‌فرستادند. با اولین حمله به بغداد، عرب‌ها از طریق پیام‌رسانی ضدجنگ برای کمپانی‌های آمریکایی و انگلیسی با آنها برخورد کردند، بدین ترتیب در کنار جنگ نظامی، جنگ هکرها نیز به‌وجود آمد.

---

1. Satellite Pictures
2. Screen Server

فصل سوم

۱ـ۳ـ جرائم رایانه‌ای و اینترنتی[1]

مقدمه انقلاب فناوری اطلاعات[2] به‌طور بنیادین جوامع را دستخوش تغییر و تحول کرده است و اکنون به سختی می‌توان بخش‌هایی از جامعه را یافت که تحت تأثیر آن قرار نگرفته باشند.

ویژگی برجسته فناوری اطلاعات، تأثیری است که بر تکامل فناوری ارتباطات راه دور گذاشته و خواهد گذاشت. ارتباطات کلاسیک[3] همچون انتقال صدای انسان، جای خود را به مبادله مقادیر وسیعی از داده‌ها، صوت، متن، موزیک، تصاویر ثابت و متحرک داده است. این تبادل و تکامل نه تنها بین انسان‌ها بلکه مابین انسان‌ها و کامپیوترها و همچنین بین خود کامپیوترها نیز وجود دارد. استفاده وسیع از پست الکترونیک و دستیابی به اطلاعات از طریق وب سایت‌های متعدد در اینترنت، نمونه‌هایی از این پیشرفت‌ها هستند که جامعه را به‌طور پیچیده‌ای دگرگون ساخته‌اند.

سهولت در دسترسی و جست‌وجوی اطلاعات[4] موجود در سیستم‌های کامپیوتری توأم با امکانات عملی نامحدود در مبادله و توزیع اطلاعات، بدون توجه به فواصل جغرافیایی، منجر به رشد سرسام‌آور مقدار اطلاعات موجود و آگاهی که می‌توان از آنها به‌دست آورد، شده است. اطلاعات، موجب افزایش تغییرات اجتماعی و اقتصادی پیش‌بینی نشده‌ای گردیده است،

1. Internet and Computer Crimes
2. Information Technology Revolution
3. Classic Communications
4. Search for Information

اما پیشرفت‌های مذکور حائز جنبه خطرناکی نیز می‌باشند که پیدایش انواع جدید جرائم و همچنین بهره‌برداری از فناوری جدید در ارتکاب جرائم سنتی بخشی از آن به‌شمار می‌رود. به‌علاوه عواقب و پیامدهای رفتار مجرمانه می‌تواند خیلی بیشتر از قبل و دور از تصور باشد، چرا که محدودیت‌های جغرافیایی یا مرزهای ملی آنرا محدود نمی‌کنند. فناوری جدید، مفاهیم قانونی موجود را دچار چالش‌هایی ساخته است. اطلاعات و ارتباطات راه دور به آسان‌ترین وجه در جهان جریان پیدا کرده و مرزها دیگر موانعی بر سر این جریان به‌شمار نمی‌روند. جنایتکاران.غالباً در مکان‌هایی به غیر از نقاطی که آثار و نتایج اعمال آنها ظاهر می‌شود، قرار دارند.

سوءاستفاده گسترده مجرمان، به‌ویژه گروه‌های جنایتکار سازمان‌یافته، از فناوری اطلاعات سبب گشته است تا سیاستگذاران جنایی اغلب کشورهای جهان با استفاده از ابزارهای سیاست جنایی درصدد مقابله با آنها برآیند. تصویب کنوانسیون جرائم رایانه‌ای در اواخر سال ۲۰۰۱ و امضای آن توسط ۳۰ کشور پیشرفته، تصویب قوانین مبارزه با جرائم رایانه‌ای توسط قانونگذاران داخلی و تشکیل واحدهای مبارزه با جرائم رایانه‌ای در سازمان پلیس بیشتر کشورهای پیشرفته و تجهیز آنها به جدیدترین سخت‌افزارها و نرم‌افزارهای کشف این‌گونه جرائم و جذب و به‌کارگیری بهترین متخصصان در واحدهای مذکور، بخشی از اقدامات مقابله‌ای را تشکیل می‌دهد.

۲ـ۳ـ پیدایش جرائم کامپیوتری

در مورد زمان دقیق پیدایش جرم کامپیوتری نمی‌توان اظهارنظر قطعی کرد. این جرم، زاییده تکنولوژی اطلاعاتی و انفورماتیکی است، بنابراین به‌طور منطقی پس از گذشت مدت کوتاهی از شیوع و کاربرد تکنولوژی اطلاعات باب سوءاستفاده نیز قابل طرح است. شیوع استعمال این تکنولوژی و برابری کاربران آن حداقل در چند کشور مطرح جهان به‌صورت گسترده، امکان بررسی اولین مورد را دشوار می‌سازد. در

نهایت آنچه مبرهن است اینکه در جامعه آمریکا، قضیه رویس موجب شد تا برای اولین‌بار اذهان متوجه سوءاستفاده‌های کامپیوتری گردند.

قضیه رویس

«الدون رویس»[1]، حسابدار یک شرکت بود و چون به‌نظر وی شرکت حق او را پایمال کرده بود، بنابراین با تهیه برنامه‌ای، قسمتی از پول‌های شرکت را به خود اختصاص داد. انگیزه رویس در این کار انتقام‌گیری بود.

مکانیزم کار بدین‌گونه بود که شرکت محل کار وی یک عمده‌فروش میوه و سبزی بود که محصولات متنوعی را از کشاورزان خریداری می‌کرد و با استفاده از تجهیزات خود از قبیل کامیون‌ها، انبار، بسته‌بندی و سرویس‌دهی به گروه‌های فروشندگان، آنها را عرضه می‌کرد. به‌دلیل وضعیت خاص این شغل، قیمت‌ها در نوسان بود و ارزیابی آنها تنها از عهده کامپیوتر برمی‌آمد تا کنترل محاسبات این شرکت عظیم را عهده‌دار شود. کلیه امور حسابرسی و ممیزی اسناد و مدارک و صورتحساب‌ها به‌صورت اطلاعات مضبوط در نوارهای الکترونیکی[2] بود.

رویس در برنامه‌ها، دستورالعمل‌ها اضافی را گنجانده بود و قیمت کالاها را با ظرافت خاصی تغییر می‌داد. با تنظیم درآمد اجناس، وی مبلغی را کاهش می‌داد و مبالغ حاصله را به حساب‌های مخصوص واریز می‌کرد. سپس در زمان‌های خاص، چکی به نام یکی از ۱۷ شرکت جعلی و ساختگی خودش صادر و مقداری از مبالغ را برداشت می‌کرد. بدین ترتیب وی توانست در مدت ۶ سال بیش از یک میلیون دلار برداشت کند. اما او در سر راه خود مشکلی داشت و آن این بود که نمی‌توانست مکانیسمی برای توقف عملکرد سیستم بیندیشد، بنابراین در نهایت خود را به مراجع قضایی معرفی و به جرم خود اعتراف کرد و به مدت ۱۰ سال به زندان محکوم شد و از اینجا بود که مبحث جدیدی به نام جرم کامپیوتری مطرح گشت.

1. Eldone Roise

2. Electronic Ribbons

۳-۳- تعریف جرم رایانه‌ای[1]

تاکنون تعاریف گوناگونی از جرم رایانه‌ای از سوی سازمان‌ها، متخصصان و برخی قوانین ارائه شده که وجود تفاوت در آنها بیانگر ابهامات موجود در ماهیت و تعریف این تیپ از جرائم است.

جرم کامپیوتری یا جرم در فضای مجازی[2] دارای دو معنا و مفهوم است. در تعریف مضیق، جرم کامپیوتری صرفاً عبارت از جرائمی است که در فضای سایبر رخ می‌دهد. از این نظر جرائمی مانند هرزه‌نگاری[3]، افترا، آزار و اذیت و سوءاستفاده از پست الکترونیک و سایر جرائمی که در آنها کامپیوتر به‌عنوان ابزار و وسیله ارتکاب جرم به‌کار گرفته می‌شود، در زمره جرم کامپیوتری قرار نمی‌گیرند.

در تعریف موسع از جرم کامپیوتری هر فعل و ترک فعلی که «در» یا «از طریق» یا «به کمک» یا از طریق اتصال به اینترنت، چه به‌طور مستقیم یا غیرمستقیم، رخ می‌دهد و توسط قانون ممنوع گردیده و برای آن مجازات درنظر گرفته شده است، جرم کامپیوتری نامیده می‌شود. بر این اساس جرائم کامپیوتری را می‌توان به سه دسته تقسیم نمود:

دسته اول: جرائمی هستند که در آنها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شوند، مانند سرقت، تخریب و غیره.

دسته دوم: جرائمی هستند که در آنها کامپیوتر به‌عنوان ابزار وسیله توسط مجرم برای ارتکاب جرم به‌کار گرفته می‌شود.

دسته سوم: جرائمی هستند که می‌توان آنها را جرائم کامپیوتری محض نامید. این نوع از جرائم کاملاً با جرائم کلاسیک تفاوت دارند و در دنیای مجازی به وقوع می‌پیوندند، اما آثار آنها در دنیای واقعی ظاهر می‌گردد، مانند دسترسی غیرمجاز به سیستم‌های کامپیوتری.

---

1. Cyber Crimes
2. Cyber Space
3. Dissolute Writing

۴ـ۳ـ طبقه‌بندی جرائم رایانه‌ای

طبقه‌بندی‌های متفاوتی از جرائم کامپیوتری توسط مراجع مختلف انجام گرفته است. برای آشنایی با آنها به ذکر موارد مهم به شرح زیر می‌پردازیم:

۱. طبقه‌بندی OECD

در سال ۱۹۸۳ (OECD) مطالعه امکان‌پذیری اعمال بین‌المللی و هماهنگی قوانین کیفری را به‌منظور حل مسئله جرم یا سوءاستفاده‌های کامپیوتری متعهد شد. این سازمان در سال ۱۹۸۶، گزارشی تحت عنوان «جرم کامپیوتری، تحلیل سیاست‌های قانونی» منتشر ساخت که به بررسی قوانین موجود و پیشنهادات اصلاحی چند کشور عضو پرداخته و فهرست حداقل سوءاستفاده‌هایی را پیشنهاد کرده بود که کشورهای مختلف باید با استفاده از قوانین کیفری، مشمول ممنوعیت و مجازات قرار دهند. بدین‌گونه اولین تقسیم‌بندی از جرائم کامپیوتری در سال ۱۹۸۳ ارائه شد و طی آن ۵ دسته اعمال را مجرمانه تلقی و پیشنهاد کرد این ۵ دسته عبارت است از:

الف) ورود[1]، تغییر[2]، پاک کردن[3] و یا متوقف‌سازی داده‌های کامپیوتری[4] و یا برنامه‌های کامپیوتری[5] که به‌طور ارادی با قصد انتقال غیرقانونی وجوه و یا هر چیز باارزش دیگر، صورت گرفته باشد.

ب) ورود، تغییر، پاک کردن و یا متوقف‌سازی داده‌های کامپیوتری و یا برنامه‌های کامپیوتری که به‌صورت عمدی و به قصد ارتکاب جعل انجام شده و یا هرگونه مداخله دیگر در سیستم‌های کامپیوتری که به‌صورت عمدی و با قصد جلوگیری از عملکرد سیستم کامپیوتری و یا ارتباطات صورت گرفته باشد.

---

1. Entrance
2. To Change
3. Delete
4. Blocking of Computer Data
5. Computer Programs

ج) ورود، تغییر، پاک کردن و یا متوقف‌سازی داده‌های کامپیوتری و یا برنامه‌های کامپیوتری.

د) تجاوز به حقوق انحصاری مالک یک برنامه کامپیوتری حفاظت‌شده با قصد بهره‌برداری تجاری از آن برنامه‌ها و ارائه آن به بازار.

ه (دستیابی[1] یا شنود[2] در یک سیستم کامپیوتری و یا ارتباطی که آگاهانه و بدون کسب مجوز از فرد مسئول سیستم مزبور چه با تخطی از تدابیر امنیتی و چه با هدفی غیرشرافتمندانه صورت گرفته باشد. توضیح یک نکته ضروری است و آن اینکه این لیست به‌دلیل عدم تفکیک جرائم و نقض تبعی اصل قانونی بودن و ابهام در ماهیت هر جرم مورد تبعیت قرار نگرفت.

۲. طبقه‌بندی شورای اروپا

کمیته منتخب جرائم کامپیوتری شورای اروپا، پس از بررسی نظرات (OECD) و نیز بررسی‌های حقوقی ـ فنی دو لیست تحت عناوین لیست حداقل و لیست اختیاری را به کمیته وزرا، پیشنهاد داد و آنان نیز تصویب کردند. این لیست‌ها به شرح زیر هستند:

لیست حداقل جرائم ضروری برای یکپارچه کردن سیاست جنایی تقنینی درباره جرم کامپیوتری:

الف. کلاهبرداری کامپیوتری[3]؛

ب. جعل کامپیوتری[4]؛

ج. خسارت زدن به داده‌های کامپیوتری[5] یا برنامه‌های کامپیوتری؛

د. دستیابی غیرمجاز[6]؛

ه . ایجاد مجدد و غیرمجاز یک برنامه کامپیوتری حمایت شده و ایجاد مجدد غیرمجاز یک توپوگرافی.

---

1. Access
2. Hearing
3. Computer Fraud
4. Computer Forging
5. Damage to Data
6. Illegal Access

لیست اختیاری:

الف. تغییر داده‌های کامپیوتری و یا برنامه‌های کامپیوتری؛

ب. جاسوسی کامپیوتری[1]؛

ج. استفاده غیرمجاز از کامپیوتر؛

د. استفاده غیرمجاز از برنامه کامپیوتری حمایت شده.

۳. طبقه‌بندی اینترپول

سال‌هاست که اینترپول[2] در مبارزه با جرائم مرتبط با فناوری اطلاعات فعال می‌باشد. این سازمان با بهره‌گیری از کارشناسان و متخصصان کشورهای عضو، اقدام به تشکیل گروه‌های کاری در این زمینه کرده است. رؤسای واحدهای مبارزه با جرائم کامپیوتری، کشورهای باتجربه عضو سازمان در این گروه کاری گردهم آمده‌اند.

گروه‌های کاری منطقه‌ای در اروپا، آسیا، آمریکا و آفریقا مشغول به‌کارند و زیرنظر کمیته راهبردی جرائم فناوری اطلاعات، مستقر در دبیرخانه کل اینترپول فعالیت می‌نمایند.

گروه کار اروپایی اینترپول با حضور کارشناسان هلند، اسپانیا، بلژیک، فنلاند، فرانسه، آلمان، ایتالیا، سوئد و انگلیس در سال ۱۹۹۰ تشکیل شد. این گروه هر سال، ۳ بار تشکیل جلسه می دهد که در ژانویه سال ۲۰۰۱ سی‌امین گردهمایی آن در دبیرخانه کل تشکیل گردید. تهیه کتابچه راهنمای پی‌جویی جرائم کامپیوتری، کتاب و سی‌دی راهنمای جرائم کامپیوتری، تشکیل دوره‌های آموزشی برای نیروهای پلیس در طول ۵ سال گذشته، تشکیل سیستم اعلام خطر که مرکب از: سیستم‌های پاسخ‌گوی شبانه‌روزی[3]، نقاط تماس دائمی شبانه‌روزی[4]، تبادل پیام بین‌المللی[5] در قالب فرم‌های استاندارد در زمینه جرائم کامپیوتری واقعه می‌باشد و انجام

1. Computer Spying
2. Interpol
3. All the Time Answering Systems
4. All the Time Point of Contact
5. Interchange International Message

چندین پروژه تحقیقاتی پیرامون موضوعات مرتبط با جرائم کامپیوتری از جمله اقدامات گروه کاری مذکور می‌باشد.

گروه کار آمریکایی جرائم مرتبط با تکنولوژی اطلاعات، مرکب از کارشناسان و متخصصان پلیس کشورهای کانادا، ایالات‌متحده، آرژانتین، شیلی، کلمبیا، جامائیکا و باهاماس است.

گروه کار آفریقایی جرائم مرتبط با تکنولوژی اطلاعات مرکب از کارشناسان آفریقای جنوبی، زیمبابوه، نامیبیا، تانزانیا، اوگاندا، بوتسوانا، سوازیلند، زنگبار، لسوتو و رواندا است که در ژوئن سال ۱۹۹۸ تشکیل گردید. این گروه فعالیتشان را با برگزاری یک دوره آموزشی آغاز نمودند و دومین دوره آموزشی آنها با مساعدت مالی سفارتخانه‌های انگلیس و فرانسه برگزار شد.

گروه کاری جنوب اقیانوس آرام و آسیا در نوامبر سال ۲۰۰۰ در هند تشکیل شد که کارشناسانی از کشورهای استرالیا، چین، هنگ‌کنگ، هند، ژاپن، نپال و سریلانکا عضو آن هستند. این گروه کاری با الگو قرار دادن کمیته راهبردی جرائم مربوط به فناوری اطلاعات به‌منظور ایجاد و هماهنگی میان اقدامات گروه‌های کاری منطقه‌ای در محل دبیرخانه کل اینترپول تشکیل گردیده است.

سازمان پلیس جنایی بین‌المللی جرائم کامپیوتری را به شرح زیر طبقه‌بندی کرده است:

۱. *دستیابی غیرمجاز*

۱ـ۱. نفوذ غیرمجاز؛

۱ـ۲. شنود غیرمجاز؛

۱ـ۳. سرقت زمان کامپیوتر.

۲. *تغییر داده‌های کامپیوتری*

۲ـ۱. بمب منطقی[1]؛

1. Logical Bomb

۲ـ۲. اسب تروا[1]؛

۲ـ۳. ویروس کامپیوتری؛

۲ـ۴. کرم کامپیوتری.

۳. کلاهبرداری کامپیوتری

۳ـ۱. صندوق‌های پرداخت[2]؛

۳ـ۲. جعل کامپیوتری؛

۳ـ۳. ماشین‌های بازی؛

۳ـ۴. دست‌کاری‌ها در مرحله ورودی/ خروجی؛

۳ـ۵. ابزار پرداخت (نقطه فروش)؛

۳ـ۶. سوءاستفاده تلفنی[3].

۴. تکثیر غیرمجاز[4]

۴ـ۱. بازی‌های کامپیوتری؛

۴ـ۲. نرم‌افزارهای دیگر؛

۴ـ۳. توپوگرافی نیمه‌هادی.

۵. سابوتاژ کامپیوتری

۵ـ۱. سخت‌افزار؛

۵ـ۲. نرم‌افزار.

۶. سایر جرائم کامپیوتری

۶ـ۱. سیستم‌های تابلوی اعلانات الکترونیک؛

۶ـ۲. سرقت اسرار تجاری؛

۶ـ۳. سایر موضوعات قابل تعقیب.

---

1. Trojan
2. Payment Cashes
3. Telephony Abuse
4. Illegal Increasing

۴. طبقه‌بندی در کنوانسیون جرائم سایبرنتیک

کنوانسیون بوداپست در اواخر سال ۲۰۰۱ به امضای ۳۰ کشور پیشرفته رسید که وظایف آن به شرح ذیل می‌باشد:

الف) هماهنگ کردن ارکان تشکیل‌دهنده جرم در حقوق جزای ماهوی داخلی کشورها و مسائل مربوطه در بخش جرائم سایبراسپیس.

ب) فراهم آوردن اختیارات لازم آئین دادرسی کیفری داخلی برای پی‌جویی و تعقیب چنین جرائمی علاوه بر جرائم دیگر که با استفاده از سیستم‌های کامپیوتری ارتکاب می‌یابند.

ج) تدوین سیستم سریع و مؤثر همکاری بین‌المللی.

کنوانسیون بین‌المللی جرائم رایانه‌ای بوداپست (۲۰۰۱) موارد زیر را جرم‌انگاری نموده است:

- نفوذ غیرمجاز به سیستم‌های رایانه‌ای؛
- شنود غیرمجاز اطلاعات و ارتباطات رایانه‌ای؛
- اخلال در داده‌های رایانه‌ای؛
- اخلال در سیستم‌های رایانه‌ای؛
- جعل رایانه‌ای؛
- کلاهبرداری رایانه‌ای؛
- سوءاستفاده از ابزارهای رایانه‌ای؛
- هرزه‌نگاری کودکان[1]؛
- تکثیر غیرمجاز نرم‌افزارهای رایانه‌ای و نقض حقوق ادبی و هنری.[۶۰]

۵ـ۳ـ مال‌خری در عصر کامپیوتر

از زمانی‌که ایده اولیه تولید یک نرم‌افزار در ذهن نرم‌افزارنویسان شکل می‌گیرد، تا زمانی‌که

1. Dissolute Writing for Children

CD آن تولید می‌شود، ممکن است هفته‌ها و ماه‌های متمادی وقت صرف آن شده باشد و مهم‌تر از همه، هزینه سنگین تولید نرم‌افزار است.

با این وجود، فقط یک هفته وقت لازم است تا نرم‌افزار تولیدشده به‌صورت کپی غیرمجاز[1] در دسترس صدها و یا هزاران کاربر کامپیوتر قرار گیرد، بدون اینکه یک ریال آن عاید تولیدکننده شود. با وجودی‌که قانون حق مالکیت معنوی و فکری به تصویب رسیده و یک شعبه خاص از اداره آگاهی نیز مأمور برخورد با کپی‌کنندگان غیرمجاز نرم‌افزارهای برنامه‌های کامپیوتری شده است، اما همه روزه صدها و شاید هزاران CD مختلف نرم‌افزار در گوشه و کنار این کشور کپی شده و با قیمت ناچیزی فروخته می‌شود.

یک کارشناس نرم‌افزار معتقد است، کنترل این امر، تقریباً محال است، چون مأموران قانون و یا حتی مالکان اصلی برنامه و نرم‌افزارها نمی‌توانند تمام چهاردیواری‌های این کشور را بازرسی و کنترل نمایند.

با این وصف یک سؤال مهم همواره بی‌پاسخ مانده است و آن اینکه چگونه و از چه طریق می‌توان در مقابل چنین معضلی ایستاد؟

به‌طور قطع تا زمانی‌که پاسخ این سؤال پیدا نشود، صنعت نرم‌افزار ایران، مانند نهالی خشکیده و بی‌ثمر برای بقای خود با مرگ، دست و پنجه نرم می‌کند.

تولیدکنندگان نرم‌افزارها می‌گویند: در چنین وضعیتی به اشتغال‌زا بودن و درآمدزایی صنعت نرم‌افزار نمی‌توان امیدوار بود، چون ریسک‌پذیری آن بالا و امنیت اقتصادی و اشتغال آن بی‌نهایت پایین است.

یک کارشناس کامپیوتر نیز می‌گوید: مادامی‌که کاربران کامپیوتر درک درستی از این موضوع پیدا نکنند، هیچ‌گونه اقدامی، مؤثر نخواهد بود. در بین کاربران جوامعی که کپی‌رایت در آن رعایت می‌شود، استفاده از کپی غیرمجاز نرم‌افزار به‌عنوان یک اقدام غیراخلاقی و غیرقانونی تلقی می‌شود. به همین جهت بسیاری از آنها در درون خود یک پلیس و ناظر دارند.

---

1. Illegal Copy

او معتقد است که مردم ما واقعاً از قبح کار اطلاع ندارند و اگر می‌دانستند که استفاده از یک نرم‌افزار کپی‌شده، به‌مثابه خریدن و استفاده از یک مال مسروقه است، به‌طور قطع چنین کاری نمی‌کردند. چون اگر غیر این بود باید اکثر مردم «مال‌خر» بودند، اما در عمل چنین اتفاقی نیفتاده است.

به این دلیل که (مال‌خری) در فرهنگ عمومی مردم مترادف با استفاده نامشروع از دسترنج و سرمایه دیگران بوده و از لحاظ شرعی، اخلاقی و قانونی مردود است. اما در استفاده از نرم‌افزار این کار را می‌کنیم. این یعنی مال‌خری در عصر کامپیوتر، قانون کشور ما تاکنون در این زمینه با خلأ بسیار جدی روبرو بوده است. بدیهی است با وجود تصویب قانون کپی‌رایت، هنوز هم راهکارهای مناسب و منطقی مقابله با این معضل، ارائه نشده است. در نتیجه می‌توان از افزایش آگاهی کاربران نسبت به تبعات غیراخلاقی و غیرقانونی این اقدام به‌عنوان یک راه‌حل عاجل و مؤثر نام برد.

یک دانشجوی کامپیوتر می‌گوید: یکی از دلایل رواج استفاده از کپی‌های غیرمجاز نرم‌افزار علاوه بر عدم اطلاع کاربران از غیراخلاقی بودن این کار، توانایی پایین کاربران در خرید نرم‌افزار است.

وی همچنین بیان می‌دارد: انسان به‌طور طبیعی در پی تهیه ملزومات و مایحتاج خود با نرخ ارزان‌تر است و کپی‌کنندگان غیرمجاز نرم‌افزار از این موضوع به راحتی سوءاستفاده می‌کنند. در حالیکه اگر شرایطی فراهم می‌شد تا کاربران بتوانند با نرخ‌های ارزان‌تر و در حد توان مالی و اقتصادی خود به نرم‌افزار دسترسی داشته باشند به‌طور قطع، استفاده از نرم‌افزارهای کپی شده تا حد قابل ملاحظه‌ای کاهش می‌یافت. این اظهارنظر بسیار منطقی است. چراکه کاربران اگر در مورد آثار اخلاقی ناگوار این کار اطلاعات چندانی ندارند، حداقل از این قدرت تشخیص برخوردارند که نرم‌افزارهای کپی‌شده از کیفیت بسیار پایینی نسبت به اصل آن برخوردار هستند.

در نتیجه مضاف بر آگاهی‌رسانی و افزایش سطح فرهنگ عمومی، استفاده صحیح از

محصولات فکری نظیر نرم‌افزار باید از ارائه راهکارهای اقتصادی جهت هماهنگی نرخ تولیدات نرم‌افزاری با قدرت خرید کاربران به‌عنوان یک رهیافت دیگر نام برد.(۶۱)

دزدی دیجیتالی[1] در اینترنت

پیش از آنکه بخش دوم فیلم جنگ ستارگان[2] به‌طور رسمی اکران شود، نسخه غیرقانونی آن در اینترنت پخش شد که به راحتی از طریق گروه‌های خبری و نامه‌های الکترونیکی Spam قابل دریافت بود.

امروزه کار قاچاق فیلم بسیار آسان شده و تنها با وسایل ساده‌ای چون یک دوربین کوچک و یک DVD-R می‌توان هزاران کپی از یک فیلم را ایجاد کرد. بنابراین جای هیچ تعجبی ندارد که شرکتی مانند سونی، آلبوم موسیقی فیلم جنگ ستارگان II را به‌گونه‌ای ساخته است که توسط کامپیوترهای شخصی قابل خوانده شدن نیست.

غیرقابل پخش بودن CDها در کامپیوترهای شخصی در پشت جعبه آنها نوشته شده و هر شخصی می‌داند که کپی کردن آهنگ‌های این آلبوم بر روی دیسک سخت کامپیوتر کار دشواری است.

البته این مسئله با نارضایتی طرفداران موسیقی نیز همراه شده است. اما شرکت سونی[3] به‌عنوان یکی از شرکت‌های عمده در زمینه پخش موسیقی چاره‌ای جز این ندارد، زیرا دزدی فیلم‌ها و آهنگ‌ها روزبه‌روز آسان‌تر می‌شود و شرکت‌ها ناچارند در مقابل این موضوع واکنش نشان دهند و در این میان، آزادی افراد تا حدودی محدود می‌گردد. به عقیده آدام لیورج[4]، سخنگوی گروه Universal Music باید جلوی دزدی دیجیتالی گرفته شود. بسیاری از همکاران لیورج از شرکت‌های مهم ضبط موسیقی چون سونی، وارنر بروس، بی.ام.ج و ... با او هم عقیده‌اند.

---

1. Digital Thief
2. Stars War
3. Sony Company
4. Addam Liory

این شرکت‌ها وضعیت اقتصادی خود را با دزدی‌های آثار موسیقی و امکان انتقال و دریافت فایل‌ها از اینترنت در خطر می‌بینند. مسلماً امروزه و در قرن بیست و یکم، PC جایگزین دستگاه‌های ضبط صوت و کاست‌ها شده است. اما PCها صرفاً امکان ضبط اطلاعات را فراهم می‌کنند و به این نکته که آیا کاربر اجازه چنین کاری را دارد، یا خیر توجهی نمی‌کنند.

در حقیقت با داشتن اینترنت، یک CD-R و یا DVD-R هر خانه‌ای به پایگاه انتشار کپی‌های فیلم و موسیقی تبدیل می‌شود.

البته بسیاری از شرکت‌های سازنده این سیستم‌ها با وجود تبلیغات قابلیت‌هایی، چون کپی کردن سیستم‌ها، به کاربران هشدار می‌دهند تا از این وسایل به درستی استفاده کنند. اما کسی نمی‌تواند اطمینان دهد که از برنامه‌هایی چون Windows Media Player شرکت مایکروسافت و iTunes شرکت اپل به‌طور قانونی استفاده می‌شود.

هر دو سی دی یک کپی غیرقانونی

به گفته سازمان بین‌المللی صنعت ضبط صدا (IFPI) اگر از هر دو CD فروخته شده در جهان، یک کپی غیرقانونی ایجاد شود، میزان فروش CD پنج درصد کاهش پیدا می‌کند، این در حالی است که فروش CD-R در سال گذشته افزایش داشت.

البته به عقیده بسیاری از محققان، افرادی که از برنامه‌های مبادله فایلی چون KazaA،Audiogalaxy، Musiccity و Morpheus استفاده می‌کنند، تمایل بیشتری برای خرید CD نسبت به دیگر افراد دارند. اما نمی‌توان این واقعیت را انکار کرد، در صورتی‌که امکان دریافت مجانی فایل‌های موسیقی فراهم باشد، دیگر کسی به‌دنبال خرید CD نمی‌رود. این مسئله‌ای است که موجب واکنش شرکتی چون سونی شده و CDهای جدید ضدکپی جنگ ستارگان در انگلستان انتشار یافته است.

در این CDها از تکنولوژی Key2audio استفاده شده و دارای اطلاعات اضافی هستند که مانع اجرای آنها توسط کامپیوترهای خانگی و Mac می‌شود. البته جاناتان موریس، رئیس بخش

ارتباطات سونی تأکید می‌کند که CD جنگ ستارگان II اولین CD ضدکپی این شرکت نیست. سونی پیش از این در انگلستان چندین آلبوم از هنرمندان معروف منتشر کرده که غیرقابل کپی هستند. در کل حدود چهار درصد از CDهای شرکت سونی ضدکپی است. این میزان با توجه به جدی بودن خطر دزدی بسیار کم به‌نظر می‌رسد و دلیل آن احتیاط شرکت سونی است.

در سال گذشته کمپانی BMG که از تکنولوژی ضدکپی استفاده می‌کرد به‌علت انتشار آلبوم White Lilies Island با دردسر مواجه شد که دلیل آن اعلام نکردن ضدکپی بودن CDها بود.

شرکت BMG عقیده دارد که هنگام انتشار آزمایش یک CD ضدکپی در صورت آگاهی مردم نمی‌توان مشخص کرد که آیا این نوع CD به پخش‌کننده‌ها آسیب وارد می‌کند یا خیر. در حقیقت یک CD هنگامی استاندارد است که با تمام پخش‌کننده‌ها قابل پخش باشد و در غیر این صورت انتشار آن برخلاف قانون است. شرکت سونی که مایل نیست دردسر مشابهی را تجربه کند، CDهای ضدکپی خود را بدون علامت آشنای Compact Disc DigitalAudio عرضه می‌کند.

جاناتان موریس اعتراف می‌کند که CDهای جدید باعث ناامیدی مشتریانی که به کامپیوتر وابسته‌اند، می‌شود. اما تاکنون این شرکت با شکایتی روبرو نشده است. شرکت‌های BMG و Universal نیز میزان CDهای برگشتی نسبت به میلیون‌ها CD منتشرشده در اروپا را بسیار ناچیز می‌دانند. این دو شرکت در ساخت CD ضدکپی از روشی به نام Shield Cactus Data که ساخته متخصصان اسرائیلی شرکت Midbar است، استفاده می‌کنند.

در این روش با استفاده از یک برنامه اضافه شده می‌توان CDها را خواند، اما امکان کپی کردن آنها وجود ندارد. البته به این ترتیب از کیفیت صدا کاسته می‌شود، اما این موضوع برای بسیاری از کاربران بی‌اهمیت است. ولی آن دسته از کاربرانی که به ایجاد کپی‌های Mp3 از CDها دلخوش دارند، ناامید می‌شوند.

در حقیقت ایجاد کپی برطبق قانون انگلستان و قوانین اتحادیه اروپا جرم محسوب می‌شود، اما این کار یک نوع امکان اضافی است که کاربران به آن عادت کرده‌اند.

حتی در صورت وجود قانون در این زمینه، رعایت کردن آن در عمل نیز مسئله‌ساز است. به‌عنوان مثال قانون کپی‌رایت و استفاده از کدها برای محافظت از برنامه‌ها، مورد قبول همگان است، اما در عمل مشکلات فراوانی را به‌وجود آورده، به‌طوری‌که اخیراً یک برنامه درس روسی در آمریکا برای شکستن کدهای مورد استفاده در برنامه Adobe که برای محافظت از کتاب‌های الکترونیکی ایجاد گشته، متهم شده است. عمل این برنامه‌نویس، تحت قانون Digital Millennium Copyright Act یک نوع فرار از تکنولوژی محسوب شده و جرم است.

همچنین مورد مشابهی درباره انتشار کدهای نرم‌افزار Decss در مجله The Quarterly Hacker منتشر شده بود. در این مجله، یک برنامه‌نویس پانزده ساله، روش کپی کردن DVD بر روی دیسک سخت کامپیوتر را به طریقی که توسط سیستم عامل لینوکس قابل اجرا باشد، توضیح داده است.

در حقیقت Decss، امکان بی‌اثر کردن سیستم محافظتی CSS را فراهم می‌کند. سیستم CSS به قدری ساده است که به آسانی و با نوشتن هفت خط، کد شکسته می‌شود و این عمل کاملاً مخالف قانون DMCA است. در اروپا نیز قانون‌شکنی‌های مشابهی در مورد قانون حمایت از کپی‌رایت (EUCD) دیده می‌شود.

به این ترتیب به‌نظر می‌رسد که این قوانین تنها در سطح بازار کارآمد بوده و نیاز مردم را برآورده نمی‌کند و شرکت‌هایی که در این زمینه فعالیت می‌کنند، خود باید قانون کپی‌رایت و استفاده عادلانه را تعریف کنند تا حقوق مشتریان و نیاز سازندگان درنظر گرفته شود و پیش از انجام چنین کاری لازم است که شرکت‌هایی چون سونی دست به‌عمل زده و به‌جای آن CDهای ضدکپی تولید کنند.

سونی در نظر دارد میزان تولید این CDها را افزایش دهد و BMG نیز تصمیم مشابهی را آغاز کرده است، همچنین تا پایان سال تمام انتشارات پاپ شرکت Universal نیز ضدکپی خواهند شد.

پیش‌بینی پایان این جنگ بسیار سخت است و شاید همچنان که انتشار جنگ ستارگان II نشان داد، پایان دادن به دزدی دیجیتالی هم کاری غیرممکن باشد.(۶۲)

۶ـ۳ـ رمزشکنان[1]

معمولاً نام رمزها برای حساب‌های کاربری (User accounts)، در یک سیستم فایل و به‌صورت رمزگذاری شده ذخیره می‌شوند و از آنجا، این اسم رمز به‌صورت کلیدی برای رمز گذاشتن بر روی بلوک مشخصی از داده‌ها به‌کار برده می‌شود. اگر هکرها بتوانند به این فایل دسترسی پیدا کنند، می‌توانند با استفاده از یک نرم‌افزار مانند Crack یا Lopht Crack آن اسم رمز را بشکنند. این برنامه‌ها، کاری را انجام می‌دهند که به نام «حمله به فرهنگ لغت»[2] معروف است. آنها هر لغت موجود در یک فرهنگ لغت را برمی‌دارند و آنرا به‌عنوان کلید برای رمزگشایی بلوک معینی از داده‌ها به‌کار می‌برند و سپس نتیجه را با یک مدخل در فایل اسم رمز مقایسه می‌کنند. اگر آنها تطبیق داده شوند در آن صورت کلمه مورد نظر، اسم رمز مطلوب برای آن حساب خواهد بود. علاوه بر کلمات فرهنگ لغت، برنامه می‌تواند از الگوهایی که به‌صورت متداول مورد استفاده قرار می‌گیرند، بهره گیرد، مانند اسامی که املای معکوسی دارند یا توالی حروف بر روی صفحه کلید مثلاً حروف «asdp» در زبان انگلیسی. کرم اینترنتی تلاش می‌کند تا اسم رمز حساب‌های کاربری را از طریق امتحان کردن نام کاربری، جابجایی ترتیبات آن و سپس فهرستی از ۴۳۲ اسم رمز جاسازی شده و در نهایت تمام کلمات موجود در یک لغت‌نامه موجود را بشکند. بیش از ٪۵۰ اسم رمزهای موجود در بعضی از سایت‌های آلوده شده[3] با این روش می‌شکنند.(۶۳)

شکستن اسم رمز، موفقیت‌آمیز است زیرا بسیاری از کاربران، اسم رمزهای ضعیفی را انتخاب می‌کنند. دو کارشناس با تحلیل و بررسی ۲۴ فایل اسم رمز جداگانه، متوجه شدند که

---

1. Password Crackers
2. Dictionary Attack
3. Infected Site

$\frac{1}{3}$ آنها حداقل یک حساب بدون هیچ‌گونه اسم رمزی دارند و بعد از اجرای برنامه Crack روی یکی از ایستگاه‌های Sun، به مدت ۱۰ دقیقه، ۵۰ اسم رمز دیگر به خطر افتادند. ۴۰ مورد دیگر، در عرض ۲۰ دقیقه بعدی و یک اسم رمز ریشه‌ای در عرض یک ساعت پیدا شدند. بعد از چند روز شکستن اسم رمز، آنها حداقل یک اسم رمز در ۱۹ فایل از ۲۴ فایل (٪۸۰)، ۵ اسم رمز ریشه‌ای و ۲۵۹ اسم رمز (٪۱۶) از تمام اسم رمزها را به‌دست آوردند. نظرسنجی انجام شده از طرف شرکت Intrusion Detection در سال ۱۹۹۵ از ۱۷۲ سایت کامپیوتری مشخص ساخت که ٪۲۳ سیستم‌ها دارای اسم رمزی هستند که به آسانی می‌توان حدس زد و ٪۲۱ به‌هیچ عنوان اسم رمز درخواست نمی‌کنند.(۶۴)

یکی از قوی‌ترین برنامه‌های رمزشکن به نام Lopht Crack از شرکت صنایع سنگین Lopht است. این ابزار دارای یک sniffer شبکه، یک تابع برای استخراج اسم رمزهای به رمز درآمده از روی دیسک یا نوار پشتیبان[1] و توانایی شکستن ۱۰ هزار اسم رمز در آن واحد می‌باشد.(۶۵) این برنامه شاخصه‌ای نیز برای ذخیره کردن مواردی که صددرصد کامل نشده‌اند، دارد تا بتوان بعدها کار را دوباره شروع کرد. این برنامه به‌صورت یک پردازش پس‌زمینه اجرا می‌شود و این توانایی را دارد که به‌طور کامل مخفی شده و با یک کلید ترکیبی[2] (Ctrl-Alt-L) دوباره آغاز گردد. Sniffer آن اقدام به جمع‌آوری اسم رمزها از سرتاسر شبکه محلی دستگاه‌های با ویندوز .N.T یا ویندوز ۹۵ که سیستم قدیمی تعیین اعتبار LAN Manager را اجرا می‌کند، می‌نماید. کاربران می‌توانند خود را با استفاده از یک سیستم تعیین اعتبار به روز شده و برنامه SYSKEY که لایه دیگری از رمزنگاری را اضافه می‌کند، محافظت نمایند.(۶۶)

در بعضی از موارد، فایل اسم رمز به‌طور مستقیم برای هرکس که بتواند وارد سیستم شود (چه به‌طور قانونی و از طریق حساب‌های خود و چه از طریق سوءاستفاده از بعضی منافذ امنیتی[3]) در دسترس است. مثلاً یک سرویس‌دهنده (Server) می‌تواند از TETP پشتیبانی کند، اما اگر

---

1. Backup Tape
2. Hot Key
3. Security Holes

پیکره‌بندی غلطی داشته باشد هرکس در هر نقطه‌ای می‌تواند هر یک از فایل‌های موجود بر روی سرویس‌دهنده را بخواند و بنویسد بدون اینکه حتی یک اسم رمز بدهد. فرد مهاجم می‌تواند از راه دور، پروتکل را تحریک کند و فایل اسم رمز (یا هر فایل دیگر) را بازیابی نماید.(۶۷)

در مواردی، فایل اسم رمز یا اسم رمزهای واحد را می‌توان بدون متصل شدن به کامپیوتر به‌دست آورد. در تحقیق از ۶۵۶ میزبان[1] بر روی فهرست برخوردهای یک متجاوز، مشخص شد که ۲۴ مورد از میزبان‌ها (۴٪) دارای فایل‌های اسم رمزی هستند که به راحتی قابل سرقت می‌باشند. بعضی از فایل‌های اسم رمز را می‌توان بر روی وب و با رفتن به آدرس http://target.com/ftp/etc/passwd به‌دست آورد که در آن target.com دلالت بر نام قلمرو سیستم هدف دارد و ftp/etc/passwd/ تعیین‌کننده فایل اسم رمز در دایرکتوری etc متعلق به دایرکتوری ftp می‌باشد، دیده شده که فردی صرفاً با استفاده از یک موتور جست‌وجوی وب[2] توانسته چندین اسم رمز ریشه‌ای به رمز درآمده را پیدا کند.(۶۸) این اسم رمزها از اندیس موجود در جست‌وجو به‌دست آمده‌اند، بنابراین وی مجبور نبود حتی برای بازیابی اسم رمزها به سراغ وب‌سایت‌ها برود. وی بعضی از اسم رمزها را کپی کرد و برنامه Cracker را فعال نمود و در عرض ۳۰ دقیقه یک اسم رمز ریشه‌ای را به خطر انداخت.(۶۹)

متخصصان امنیت[3] از همان ابزارهای رمزشکنی[4] استفاده می‌کنند که مورد کاربری هکرها ست تا امنیت فایل‌های اسم رمز خودشان را ارزیابی کنند. دسترسی داشتن به فایل etc/passwd لزوماً دسترسی به هر اسم رمز را فراهم نمی‌کند. اسم رمزها علاوه بر رمزدار بودن می‌توانند در «سایه»[5] باشند، یعنی در فایل دیگری ذخیره شوند که به آسانی نمی‌تواند در دسترس قرار گیرد. فایل etc/passwd هنوز وجود دارد، اما فقط حاوی اطلاعات محاسبه است نه اسم رمزها.(۷۰)

---

1. Host
2. Web Search Engine
3. Security Specialists
4. Cracking Tools
5. Shadowed

رابطه دروازه مشترک (common gateway interface=cgi) به صفحات وب امکان می‌دهد تا اجرای اسکریپت‌های ذخیره شده در دایرکتوری cgi-bin را روی سرویس‌دهنده تعیین کنند. نرم‌افزار روی سرویس‌دهنده (سرور) اجرا می‌شود (برخلاف کامپیوتر فرد کاربر) و برای پردازش فرم‌ها و جست‌وجو در بانک‌های اطلاعاتی مورد استفاده قرار می‌گیرد. نقض امنیتی موجود می‌تواند به کاربرهای دوردست امکان دهد تا اطلاعات را از سرویس‌دهنده استخراج کنند. اسکریپت‌های نمونه برای بهره‌برداری از نقطه ضعف phf در اینترنت به طور گسترده‌ای در دسترس هستند.(۷۱)

هکرها علاوه بر به‌دست آوردن اسم رمز از Sniffer و فایل‌های اسم رمز، می‌توانند آنها را به‌صورت جاسازی شده در نرم‌افزارها[1] پیدا کنند. مثلاً در فوریه سال ۱۹۹۷ در سرور اطلاعات اینترنتی مایکروسافت، نقصی پیدا شد که به هر فردی که مشغول مرور کردن وب باشد این امکان را می‌داد تا فایل‌های asp (صفحات سرویس‌دهنده فعال) را بخواند. این صفحات که حاوی کد برای اجرا شدن هستند و نه برای خواندن، ممکن است حاوی اسم رمز یا دیگر اطلاعات حساس باشند.(۷۲)

برای مرور یک صفحه بر روی دستگاه هدف[2]، تنها کاری که لازم است، کاربر انجام دهد این است که در پایان آدرس‌های وب یک نقطه تایپ کند مثلاً http://www.Victim.com/default.asp و در نتیجه مایکروسافت سریعاً این نقیصه را برطرف می‌کند.(۷۳)

سرریزشدن بافر[3] و موارد دیگر بهره‌وری

در مواقعی، هکرها بدون وصل شدن به سیستم از طریق یک حساب یا اسم رمز وارد سیستم‌ها می‌شوند. در عوض، آنها برنامه‌ای را که روی سیستم مشغول اجراست، تحریک

1. Embedded in Software
2. Target Machine
3. Buffer Overflows

می‌کنند و از آن به‌عنوان وسیله‌ای برای خوراندن کد مخربی به درون سیستم استفاده می‌کنند.[۷۴]

هکرها برای اینکه کاری کنند تا سیستم بتواند، کد خود آنان را اجرا کند، رشته بلندی از ورودی (input) را برای برنامه هدف ایجاد می‌کنند. این رشته ورودی حاوی کدهای آنان در کنار دیگر داده‌ها می‌باشد. معمولاً برنامه هدف، کدی را که به‌صورت ورودی وارد شده، اجرا نمی‌کند. اما اگر آن ورودی به قدری بلند باشد که فضای حافظه اختصاص داده شده به آنرا (به نام بافر) لبریز کند، ممکن است آن کد تحت شرایطی خاص اجرا شود. چنین امری به این علت اتفاق می‌افتد که ورودی مذکور بر روی process stack قرار داده می‌شود. این مکانی در حافظه کامپیوتر است که ردّ ورودی‌های برنامه و کد مورد استفاده برای پردازش این ورودی‌ها را نگهداری می‌کند. هرگاه کارکرد برنامه‌ای فعال شود، یک آدرس بازگشتی که به کد موردنظر اشاره دارد و قرار است هنگامی‌که آن کارکرد تکمیل شود، اجرا گردد، روی Stack قرار داده می‌شود.[۷۵] در آن صورت بافر ورودی روی آن قرار می‌گیرد. اگر داده‌های ورودی از فضای بافر سرریز شوند، روی منطقه Stack در زیر آن ریخته می‌شوند و هرچه را که قبلاً در آنجا وجود داشته Over write می‌کنند، از جمله آدرس بازگشتی. با طراحی دقیق رشته ورودی، فرد می‌تواند تنظیم کند که محل Stack حاوی آدرس بازگشتی، به کد مخرب در بافر ورودی اشاره داشته باشد. سپس این کد روی دستگاه کاربر اجرا می‌شود. علاوه بر آن، این کد با امتیازات برنامه‌ای اجرا می‌شود که مشغول بهره‌برداری از آن است. از این حمله به آسانی می‌شود، اجتناب کرد به شرطی که برنامه، اندازه ورودی خود را قبل از ارسال آن بر روی Stack بررسی کند، اما متأسفانه همه برنامه‌ها این کار را نمی‌کنند.[۷۶]

مشکلات ناشی از سرریز شدن بافر سال‌هاست که سیستم را دچار آفت کرده و در انواع برنامه‌ها مانند fingerd (برنامه finger daemon) و talked (برنامه talk daemon) خود را نشان می‌دهند. دمون‌ها برنامه‌هایی هستند که در پس‌زمینه اجرا می‌شوند و به درخواست‌های راه دور برای سرویس، پاسخ می‌دهند. مثلاً finger daemon اطلاعاتی را درباره حساب کاربر

ارائه می‌دهد. من برای پیدا کردن اطلاعاتی درباره کاربری به نام Ceo در Victim.com، فرمان finger Ceo@victim.com را تایپ می‌کنم.(۷۷) سپس برنامه finger روی دستگاه من اقدام به آغاز اتصال به fingerd process روی Victim.com می‌کند که با خود اطلاعاتی مانند نام اصلی کاربر، شماره دفتر و زمان آخرین Login را ارائه می‌کند. در حملاتی از نوع سرریزشدن بافر، هکر اقدام به ثبت صدور یک فرمان finger command با یک رشته بلند از داده‌ها می‌کند که حاوی کد مخرب است. فروشندگان با برطرف کردن مشکلات ناشی از سرریزشدن بافر در برنامه‌های fingerd و دیگر برنامه‌های سیستمی از خود واکنش نشان داده‌اند، اما تمام مشتریان این موارد تعمیری را اجرایی نمی‌کنند و مشکلات در برنامه‌های جدید و حتی مدل‌های جدید از برنامه‌های قدیمی خود را نشان می‌دهند.(۷۸)

روش‌های فوق به هیچ‌وجه جامع ابزارها و تکنیک‌هایی نیستند که در اختیار هکرها قرار دارند. بسیاری از سیستم‌ها دارای نقاط ضعفی هستند که خود را در برابر انواع تخصصی حملات رها می‌سازند. مثلاً در ژوئیه سال ۱۹۹۸ مجله Newsbytes گزارش داد که یک شرکت کوچک و نوپا به نام شرکت امنیت کامپیوتری[1] Byte Tight یک روزنه را در ویندوز شرکت مایکروسافت اعلام کرده که می‌توان از آن برای دسترسی به فایل‌های ذخیره شده بر روی یک کامپیوتر دیگر سوءاستفاده کرد. اگر هدف، کار file sharing (اشتراک فایل‌ها) را فعال کرده باشد، هکر می‌تواند به فهرستی از فایل‌های به اشتراک گذاشته شده (shared شده) روی دستگاه مورد نظر دست یابد. این کار با باز کردن کادر run در ویندوز و تایپ کردن دو back slash قبل از آدرس IP هدف انجام شده بود. اگر دسترسی کامل (full access) روی دستگاه دوردست فعال می‌بود، هکر می‌توانست هر یک از فایل‌های آنرا بخواند، اصلاح کند یا حذف نماید یا فایل‌های جدیدی را اضافه کند. این مجله اعلام کرد که آنها حمله‌ای را (با مجوز) امتحان کرده و توانسته بودند فایل جدیدی را با محتویات "Haha - kilray was here! ایجاد کنند.(۷۹) رئیس شرکت Byte Tight،

1. Computer Security Corp

مایکل پاریس[1] اعلام کرد که درصد افراد آسیب‌پذیر بر روی اینترنت، ممکن است ٪۸۰ باشد. وی همچنین بیان کرد که افراد شرکت، مشغول عمومی کردن این مسئله بوده‌اند، زیرا یکی از برنامه‌های ویندوز که کار حمله را به‌صورت خودکار درآورده بر روی یکی از وب سایت‌های هکر محبوب منتشر شده بود. بنا بر اعلام روزنامه South China Morning Post ابزاری به نام Winhack gold می‌تواند از میان هزاران کامپیوتر متصل شده به اینترنت اقدام به جست‌وجو نماید تا آنهایی را که آسیب‌پذیر هستند، پیدا کند. دانیل آیرز[2]، متخصص امنیت شبکه در شرکت ارائه دهنده خدمات اینترنتی Net Link از نیوزلند می‌گوید: «نکته وحشتناک در مورد آن، این است که به هرکس که نسبت به دسترسی به دستگاه فرد دیگری کاملاً بی‌خیال است، توانایی می‌بخشد.»(۸۰)

۷ـ۳ـ مهندسی اجتماعی[3]

هکرها در اغلب موارد از مهندسی اجتماعی برای ورود به سیستم‌های کامپیوتری استفاده می‌نمایند. ممکن است آنها وانمود کنند که یک تکنسین جدید یا مشاور امنیتی[4] هستند که نیازمند اسم رمز برای برطرف کردن یک مشکل می‌باشند، یا از افراد عالی‌رتبه‌ای[5] هستند که در دسترسی به سیستم مشکل دارند و نیازمند کمکند. ممکن است از هدف مورد نظر بخواهند تا برای آنها یک حساب کامپیوتری راه‌اندازی کند. ایرا وینکلر[6]، نویسنده کتاب «جاسوس شرکتی»[7]، در یک نظرسنجی از حاضران در جلسه DefCon به سال ۱۹۹۶، متوجه شد که مهندسی اجتماعی تشکیل‌دهنده ٪۲۰ روش‌هایی است که آنها برای نفوذ به سیستم‌های کامپیوتری مورد استفاده قرار می‌دهند.(۸۱)

وینکلر که برای شرکت‌ها و مشتریان دولتی حسابرسی امنیتی انجام می‌دهد، متوجه شد که با استفاده از ترفند توجیه امنیتی[8]، که تا حدودی به‌وسیله ترساندن کارگر می‌افتد، از کارمندان

---

1. Michael Paris
2. Daniel Ayers
3. Social Engineering
4. Security Consultant
5. High-Ranking Person
6. Ira Winkler
7. Corporate Espionage
8. Security Briefing Ruse

جدید می‌تواند اسم رمزها را دریافت کند. او با تظاهر به اینکه مدیر امنیتی است، درباره محیط سخت‌افزاری و نرم‌افزاری[1] آنها پرس‌وجو می‌کرد و قبل از سؤال آخر، سؤالات متعدد و بی‌ربطی را می‌پرسید تا نام کاربری، اسم رمز و شماره مودم آنها را به‌دست آورد. او جلسات توجیهی امنیتی را با ارائه خطوط راهنمای امنیتی ابتدایی به کارمندان به پایان می‌رساند.(۸۲)

وینکلر همچنین حادثه‌ای را از مهندسی معکوس اجتماعی[2] ذکر می‌کند که طی آن، یک هکر اوضاع را طوری مرتب کرد تا قربانیان مستقیم به سراغ او بیایند. او اعلان‌های دستی را بر روی بولتن بردهای[3] یک شرکت منتشر می‌کرد و شماره‌ای را اعلام می‌نمود. کارمندان به‌طور مرتب با این شماره تماس می‌گرفتند و اسم رمزها و دیگر اطلاعات را در ازای دریافت کمک می‌دادند. آنچه آنها نمی‌دانستند این بود که مشغول گرفتن شماره تلفن منزل هکر هستند.(۸۳)

سوزان تاندر[4]، یکی از روش‌های هک کردن خود را به کتی هافنر و جان مارکف در زمانی‌که مشغول نوشتن Cypher punk بود، بیان کرد. آن‌طور که او گفته «من در اتاقی با یک کامپیوتر و تیمی از مقامات نظامی نشسته بودم. آنها از من درخواست کردند تا از هر ابزاری که در اختیار دارم، استفاده کنم تا وارد یکی از کامپیوترهای نظامی به خصوص شوم. پس از استفاده از یک دایرکتوری سهل‌الوصول برای اینکه متوجه شوم سیستم در کجا قرار دارد، با پایگاه تماس گرفته و از دانش اصطلاحات نظامی خود استفاده کردم تا اسم افسر فرمانده در SCIF (تأسیسات اطلاعات تفکیک شده امن) را به‌دست آورم».(۸۴) بعد از اینکه به من گفتند که نام او هستینگز[5] است کمی با او گپ زدم و گفتم نمی‌توانم اسم منشی شما را به یاد آورم. «منظور شما متخصص بوکانان[6] است؟» من با تغییر لحن از بی‌اعتنایی و خونسردی به لحنی آمرانه با مراکز داده‌ها تماس گرفتم و گفتم: «متخصص بوکانان از طرف سرگرد هستینگز تماس گرفته‌ام. او مشغول تلاش برای دسترسی به حساب خود بر روی این سیستم بوده، اما نتوانسته

---

1. Hardware and Software Environments
2. Reverse Social Engineering
3. Bulletin Boards
4. Susan Thunder
5. Hastings
6. Buchanan

وارد شود و می‌خواهد بداند، چرا این‌گونه شده است». وقتی اپراتور جواب داد با ناراحتی گفتم: «بسیار خوب، ببین، من نمی‌خواهم این اطراف پرسه بزنم. اسم، درجه و شماره مخصوص شما چیست؟ در عرض ۲۰ دقیقه به دستگاهی رسیدم که مدعی بودند دارای داده‌های طبقه‌بندی شده است در همین زمان سرهنگی از روی صندلی خود بلند شد و گفت: «کافی است، از شما متشکریم» و دو شاخه را کشید.[(۸۵)]

هکرها از مهندسی اجتماعی برای دسترسی به حساب‌های شرکت‌های آمریکن آنلاین[۱] (AOL) استفاده کرده‌اند. یک هکر با دانستن نام واقعی، نام ظاهری و آدرس هر یک از اعضای AOL، با خطوط پشتیبانی این شرکت تماس گرفته و نماینده خدمات مشتریان را اغوا می‌کند تا اسم رمز موجود در حساب آن فرد را دوباره تنظیم کند. در این صورت، آن هکر دسترسی انحصاری به آن حساب خواهد داشت. اطلاعات مربوط به اعضای AOL در اغلب موارد در پروفایل آنلاین آنها موجود است. این شرکت معمولاً از کاربرانی که خواهان تنظیم دوباره اسم رمز خود هستند، می‌خواهد تا اطلاعات کارت اعتباری خود را ارائه کنند، اما در این موارد خاص درخواست نکرده است.[(۸۶)]

وسایل نرم‌افزاری وجود دارند تا کار مهندسی اجتماعی را تسهیل نمایند. برنامه AOHELL، که یکی از موارد افزوده شده هکرها به نرم‌افزار America Online می‌باشد، دارای خصوصیتی است که به هکرهای AOL این امکان را می‌دهد تا از دیگر اعضای شرکت، اسم رمز و شماره کارت اعتباری را به‌دست آورند. هکر وارد یک تالار گفت‌وگو[۲] می‌شود و بعد از باز کردن فهرست افراد، پیامی مانند این را انتخاب می‌کند: «من از طرف اداره صدور صورتحساب آمریکن، آنلاین تماس گرفته‌ام. ما مشغول بررسی مشکلات موجود در سوابق خود هستیم. لازم است شما اسم رمز برقراری ارتباط خود را برای من تأیید کنید تا بتوانیم اعتبار شما را به‌عنوان یک کاربر تأیید کرده و فوراً سوابق شما را تصحیح کنیم». این پیام

1. American Online　　2. Chat room

به‌صورت یک «پیام فوری»[1] به تمامی اعضای حاضر در تالار فرستاده می‌شود. هکر از قبل مقرر کرده که پاسخ‌ها در یک Log file ذخیره شوند. برنامه دیگری به نام Toolz of Destvuction شامل ۱۸ عبارت استوک است. در بین آنها: «شما مجازید تا حساب خود را به یک حساب فوق سری انتقال دهید. این کار کاملاً رایگان است. تنها کاری که باید انجام دهید این است که اسم رمز خود را تبدیل به "Overhead" کنید و آنرا دوباره برای ما با پست الکترونیک بفرستید».(۸۷)

۸ـ۳ـ پوشاندن راه‌ها[2]

هکرها برای مخفی کردن حضور خود و پنهان داشتن مسیرهای خود چندین کار انجام می‌دهند. مثلاً اگر فایل‌هایی را ایجاد کنند ممکن است نام‌هایی نیز به آنها بدهند که با «.» شروع می‌شود تا کاری کنند که توجه به آنها خیلی محتمل نباشد. ممکن است برخی از برنامه‌های System Utility را که اطلاعات مربوط به وضعیت سیستم را نشان می‌دهد (مثلاً کدام کاربرها وصل شده‌اند و کدام برنامه‌ها در حال اجرا هستند) با مدل‌هایی تعویض کنند که فعالیت هکر را مخفی می‌کند.

معمولاً زمانی‌که کاربر وارد سیستم می‌شود یا فرمانی را صادر می‌کند یک audit record به‌وجود می‌آید و در یک Log file ذخیره می‌شود. سپس یک برنامه می‌تواند این Log را پردازش کند تا فعالیت‌های مشکوک[3] را انتخاب نماید. متجاوزان، کار حسابرسی را از فعالیت می‌اندازند یا اینکه سوابق خود را از Log file حذف می‌کنند.(۸۸)

جعبه ابزارهای نرم‌افزاری[4] وجود دارند که به این فعالیت‌ها کمک می‌کنند. برنامه‌ای به نام Root Kit شامل یک Sniffer شبکه، یک برنامه Login که کار حسابرسی را از کار می‌اندازد و مدل‌های هکری برنامه‌های متداول از جمله "ps" (وضعیت پردازش) و "netstat" (وضعیت شبکه) است.(۸۹)

---

1. Instant Message
2. Covering up Tracks
3. Suspicious Activity
4. Software Toolkits

تکنیک دیگری که مورد استفاده قرار می‌گیرد تا ردیاب‌ها (trackers) با شکست مواجه شوند به Looping معروف است. آنها به جای نفوذ مستقیم به یک سیستم معین، وارد سیستمی شده و از آن به‌عنوان تخته شیرجه[1] برای نفوذ به دیگری استفاده می‌کنند و از دومی برای نفوذ به سومی و الی آخر و در نهایت به سیستم هدف می‌رسند. تأثیرش، این است که محل فرد متجاوز مخفی بماند و هرگونه تحقیق و بازرسی با پیچیدگی‌هایی مواجه شود. ضروری است، بازرسان برای پیدا کردن سرچشمه، از مدیران سیستم در طول این راه کمک بگیرند. جلب این همکاری اگر از مرزهای ملی عبور کند، می‌تواند به طرز خاصی دشوار باشد.

در تجاوز به آزمایشگاه‌های رم، هکری به نام Data stream Cowboy که ساکن انگلستان بود از میان کامپیوترهای نیروی هوایی آمریکا به‌عنوان سکوی پرتاب اینترنتی استفاده کرده بود تا به دیگر سایت‌های نظامی و غیرنظامی سراسر دنیا نفوذ کند.(۹۰)

لوپینگ باعث می‌شود که به‌نظر رسد یک حمله در یک سایت از سایت دیگری سرچشمه گرفته است. در زمان یکی از تجاوزات او به آزمایشگاه‌های رم، بازرسان از نیواسکاتلندیارد مشغول تماشای این بودند که Data stream در حال دسترسی به سیستم مؤسسه تحقیقات اتمی کره از آزمایشگاه‌های رم و دریافت تمام داده‌های آن بر روی کامپیوتر نیروی هوایی است. در ابتدا آنها مطمئن نبودند آیا سیستم متعلق به کره شمالی است یا جنوبی، اگر اولی باشد اهالی کره شمالی می‌توانند تجاوز آشکار از نیروی هوایی آمریکا را نوعی عمل جنگی تجاوزکارانه تلقی کنند. در آن زمان آمریکا مشغول مذاکراتی حساس با کره شمالی بر سر برنامه تسلیحات هسته‌ای آنها بود. اما در عرض چند ساعت، بازرسان به این نتیجه رسیدند که سیستم متعلق به کره جنوبی است.(۹۱)

۹ـ۳ـ سرقت اطلاعات[2]

وقتی فرد متجاوز به یک حساب نفوذ می‌کند، می‌تواند هر اطلاعاتی را که برای آن

---

1. Spring Board
2. Information Theft

حساب مجاز است (از جمله پیام‌های الکترونیکی شرکتی یا خصوصی، اسناد حساس یا انحصاری[1] و بانک‌های اطلاعاتی[2]) را بخواند و down Load کند. با وجودی‌که صاحب اطلاعات هنوز به اطلاعات اولیه دسترسی دارد، ممکن است خسارت قابل ملاحظه‌ای از این امر (که معمولاً سرقت اطلاعات مفید نامیده می‌شود) حاصل گردد. فرد متجاوز می‌تواند از این اطلاعات برای مزیت مالی یا رقابتی استفاده کند، یا انواع دیگری از ناراحتی را به‌وجود آورد.

۱۰ـ۳ـ گردآوری نشان‌های افتخار[3]

ممکن است برای یک نوجوان هدفش به‌دست آوردن پول و یا ایجاد دردسر نباشد، بلکه او می‌خواهد از یک هیجان لذت ببرد و نشان‌های افتخار یعنی اسناد و اخبار داغی جمع‌آوری کند که با آنها در تالارهای گفت‌وگو یا روی بولتن بردها لاف بزند.

کریستین والور[4] بعد از ۱۷ سال در دنیای زیرزمینی کامپیوتر که به نام Se7en معروف است در DefCon IV ـ که نشست سالانه هکرها در لاس‌وگاس است ـ، ظاهر شد تا درباره هکرها صحبت کند، این افراد با مفهوم «کسب نشان‌های افتخار» آشنا هستند. ممکن است بچه‌ای وجود داشته باشد که نقشه‌های مربوط به جنگنده‌های رادارگریز را بر روی کامپیوتر خود بریزد، آنرا در یک دیسکت قرار دهد و به دیوار بچسباند که «بله من هم می‌دانم». او نمی‌خواهد اینها را به یک جاسوس بفروشد. او حتی نمی‌داند که اگر زندگی‌اش بستگی به آن داشته باشد، باید به چه کسی بفروشد. برای او، هدف این کار صرفاً نشان دادن خود او است.(۹۲)

یکی از معروف‌ترین جوایز افتخار هکری، یک سند Bell South بود که به مدیریت سیستم اضطراری ۹۱۱ تقویت شده (E911) تعلق داشت. فایل E911 در سال ۱۹۸۸ از یکی از

---

1. Proprietary or Sensitive Documents
2. Databases of Information
3. Gathering Trophies
4. Christian Valour

کامپیوترهای شرکت Bell South به‌دست رابرت ریگز[1] به سرقت رفت. ریگز که عضو گروه هکرهایی موسوم به Legion of Doom بود، این سند را به کرگ نایدروف که در آن زمان سردبیر خبرنامه الکترونیکی[2] Phrack بود، تحویل داد. نایدروف[3]، دانشجوی دانشگاه میسوری، آن را ویرایش نمود و در شماره فوریه ۱۹۸۹ منتشر کرد. ولی در سال ۱۹۹۰ وی دچار دردسر بدی شد. دفتر دادستانی آمریکا در شیکاگو او را متهم به ۱۰ فقره خلاف از کلاهبرداری سیمی و حمل و نقل درون ایالتی اموال و دزدی کرد که مجازاتش بالغ بر ۶۵ سال زندان می‌شد. قرار بود که در ۲۳ ژوئیه در شیکاگو به دادگاه رود. پس از ۴ روز دادگاه، دادستان‌های دولت اتهامات را پس گرفتند و قاضی نیکولاس‌بوا پرونده را بست. اساس این پرونده، سرقت اسرار تجاری بود و تیم مدافعان نشان دادند هر چیزی که نایدروف منتشر کرده در محدوده عمومی بوده است.(۹۳)

پرونده نایدروف، سؤالات مهمی را درباره آزادی مطبوعات و مسئولیت‌های ناشران در اینترنت مطرح کرد. اگر مطالب موجود در سند E911 در قلمرو عمومی وجود نداشتند، فردی که اسناد را امروز منتشر می‌کرد، ممکن بود به جرم نقض قانون جاسوسی اقتصادی گناهکار شناخته شود. این قانون به صراحت دریافت[4]، مالکیت[5]، کپی کردن[6]، تکثیر[7]، ارسال[8] و مکاتبه اسرار تجاری[9] را دربرمی‌گیرد. ناشر نیز ممکن بود بابت نقض قانون کپی‌رایت، تحت تعقیب قرار گیرد، زیرا این قانون افرادی را که از نقض عمدی این قانون سود نمی‌برند، مستثنی نمی‌داند.

هکرها در اغلب موارد ابزارهای نرم‌افزاری را به سرقت می‌برند تا فعالیت‌های خود را تقویت نمایند. مجله Under ground سولت درایفوس گزارشی از ماجرای دو هکر استرالیایی

---

1. Robert Riggs
2. Electronic Newsletter
3. Neidorf
4. Receipt
5. Possession
6. Copying
7. Duplication
8. Transmission
9. Communication of Trade Secrets

به نام‌های Phoenix و Electron را چاپ کرده کـه بـا اصـرار، خواهـان یـک کپـی از برنامـه Deszip بودند ـ برنامه‌ای که به‌دست یکی از کارشناسان برجسته امنیتی در آمریکا نوشته شـده است. اگر آنها می‌توانستند دسـت خـود را بـه ایـن برنامـه برسـانند، دیگـر نمـی‌شـد جلـوی استرالیایی‌ها را گرفت، چراکه قادر می‌گشتند اسم رمزها را بسیار سریع‌تـر از ابزارهـای کنـونی خود بشکنند. اما به‌دست آوردن آن کار آسانی نبود، زیرا قوانین صادراتی، توزیع این نرم‌افزار با توانمندی‌های رمزگذاری در خارج از آمریکا را بدون مجوز ممنوع می‌سـاخت. هکرهـا یکبـار توانسته بودند تا Deszip را از روی دستگاه برنامه‌نـویس آن یعنـی مـات بیـشاپ در دانـشگاه دارتموث دریافت کنند، اما فقط کشف کردند کـه خـود برنامـه رمزگـذاری شـده اسـت، ولـی نتوانستند اسم رمز آنرا بشکنند. فونیکس بالاخره نه تنها Deszip بلکه اسم رمـز آنـرا نیـز پیـدا کرد. هکرها با در دست داشتن اسم رمز، فکر می‌کردند، ممکن است بتوانند رمز نسخه دانشگاه دارتموث را باز کنند، اما آنرا پیدا نکردند. در نهایت آنهـا آنـرا از یکـی از هکرهـای انگلـستان به‌دست آوردند، اما برای از رمز درآوردن آن به کامپیوتری در ناسا وارد شده و فایل را به آنجـا انتقال دادند و در همان‌جا از رمز درآوردند تا فقط کشف کنند که این‌بار فایل تا حدودی نـابود شده است.(۹۴)

بیش از نشان افتخار

هکرها وارد کامپیوترهای شرکت‌های تلفن شده و نرم‌افزارهای حساس[1] و دیگـر اطلاعـات را بر روی کامپیوتر شخصی خود می‌ریزند.

کوین میتنیک[2] (یک هکر مشهور) تاریخچه بلنـدی از نفـوذ در کامپیوترهـا و سیـستم‌هـای تلفنی دارد. در طول دهه ۸۰ م. او در کامپیوترهای متعددی نفـوذ کـرد و سـرویس‌هـای تلفـن راه‌دور را به سرقت برد.

هکرها، شماره‌های کارت اعتباری را از روی کامپیوترهای شرکتی به‌دست می‌آوردند. حتـی

1. Sensitive Software
2. Kevin Mitnick

اگر از شماره‌های به سرقت رفته هیچ‌گاه استفاده نشود، دادوستد شماره‌های کارت و دیگر دستگاه‌ها یا کدهای دسترسی، جرم محسوب می‌شوند.[۹۵]

اسم رمز[۱] یکی از اهداف ثابت هکرها است. هکرها در مواقعی، از اطلاعات حساسی که به‌دست می‌آوردند برای هشدار به مدیران سیستم و کاربران نسبت به مشکلات امنیتی استفاده می‌کنند.

از دست دادن کنترل بر روی اسم رمزها یا دیگر اطلاعات می‌تواند اعتماد مشتری به سرویس‌های آن‌لاین را از میان ببرد. گفته می‌شود حمله به AUSNet شرکت استرالیایی ارائه‌دهنده خدمات اینترنتی، بیش از ۲ میلیون دلار از نظر از دست دادن مشتریان و قراردادها خسارت وارد آورده است.

برخی از متجاوزان از داده‌هایی که به سرقت برده‌اند، برای گرفتن حق‌السکوت از سیستمی استفاده می‌کنند که مورد نفوذ قرار داده‌اند. موارد نفوذ به کامپیوترها، ابزاری را برای جاسوسی در سطح شرکتی و ملی به‌دست می‌دهند.

بنا بر اعلام خبرنامه Intelligence News Letter در سال ۱۹۹۷، شخصی به کامپیوترهای وزارت خارجه سوئیس نفوذ کرد، از جمله کامپیوترهای متعلق به گروه ضربت که مشغول بررسی سرمایه‌های سپرده شده در حساب‌های بانک سوئیس از طرف یهودیان در قبل و بعد از جنگ جهانی دوم بودند، اما فرد متجاوز شناسایی شد.

یک گروه متشکل از ۱۵ هکر (۸ آمریکایی، ۵ انگلیسی و ۲ روسی) اعلام کردند که به کامپیوترهای ناسا نفوذ کرده‌اند. آنها مدعی بودند، نرم‌افزاری را به سرقت برده‌اند که برای دفاع در برابر متجاوزان به‌کار برده می‌شود و اینکه این اطلاعات به آنها نشان خواهد داد که چگونه بدون شناخته شدن، از میان سیستم‌های آنها عبور کنند. اما یکی از مقامات ناسا گفت: «اینها چیزهای باارزشی نیستند که یک هکر برای خود برمی‌دارد».[۹۶]

---

1. Password

۱۱ـ۳ـ دستکاری

همان‌گونه که بیان شد، متجاوزان در اغلب موارد داده‌های روی کامپیوترها را مورد نفوذ قرار می‌دهند و دستکاری می‌کنند. آنها حساب‌های تقلبی ایجاد می‌کنند که می‌توانند برای موارد بعدی Loginهای خود را مورد استفاده قرار دهند، برنامه‌های Sniffer را نصب می‌کنند تا اسم رمز و نام کاربری افراد را به‌دست آورند، ردّ خود را از روی Log file پاک می‌کنند، برنامه‌های استاندارد را برداشته و برنامه‌هایی را جای آنها می‌گذارند که حضور آنها را پنهان می‌سازد و اقدامات متعدد دیگری انجام می‌دهند تا از هک کردن‌های خود پشتیبانی نمایند.[۹۷] برخی جلوتر می‌روند و داده‌های کاربردی ذخیره شده بر روی سیستم را تغییر می‌دهند. اثر این کار نابود کردن یکپارچگی کل سیستم و داده‌هایی است که تحت تأثیر قرار می‌گیرند. هزینه این کار برای صاحبان سیستم‌ها، زمانی است که صرف احیای سیستم و داده‌ها می‌شود. ممکن است، هزینه‌های دیگری نیز با شهرت بد پیدا کردن و ناتوانی در دسترسی به داده‌های صحیح در یک دوره مورد انتظار، همراه باشند.[۹۸]

هکرها به‌طور مکرر، داده‌ها را به‌عنوان شوخی، اعتراض یا به نمایش گذاردن مهارت‌های خود دستکاری می‌کنند. فونیکس[1]، هکر استرالیایی که در جست‌وجوی برنامه Deszip وارد سیستم یوجین اسپافورد شده بود در کامپیوتر کالیف استول (فردی که هکرهای کا.گ.ب روسیه را ردیابی و کتاب تخم کوکو را نوشته بود) نیز نفوذ کرده بود. فونیکس، دسترسی ریشه‌ای بر روی دستگاه استول را پیدا کرده و پیام روز را با این جمله تغییر داده بود: «به‌نظر می‌آید که تخم پرنده کوکو به صورتش خورده است».[۹۹]

چندین مورد نیز دوباره دانش‌آموزانی گزارش شد که به کامپیوترهای مدرسه دسترسی پیدا کرده‌اند تا نمرات خود یا نمرات هم‌کلاسی‌های خود را دستکاری کنند.[۱۰۰]

یکی از زندانیان زندان سانتا کلارا کانتی[2] در کالیفرنیا وارد سیستم اطلاعات آن‌لاین[3] زندان

1. Phoenix
2. Kevin Mitnick
3. On-line Information System

شد و تاریخ آزادی خود را از ۳۱ دسامبر به ۵ دسامبر تغییر داد تا بتواند برای عید کریسمس در خانه‌اش باشد. اما زمانی‌که معاون شکاک متوجه این دستکاری شد، نتیجه عکس به‌بار آورد.(۱۰۱)

هکرها در انگلستان موارد اعلامی در ایستگاه‌های اتوبوس را تغییر داده و به‌جای اطلاعاتی که برای مردم نابینا بود، فحش‌ها و سخنان رکیک پخش می‌کردند.(۱۰۲)

۱۲ـ۳ـ هک کردن‌های وب[1]

وب سایت‌ها از اهداف مطلوب هکرها به‌شمار می‌روند و شاید دلیل آن این باشد که آنها مکرراً سطح پایینی از امنیت و سطح بالایی از مرئی بودن را ارائه می‌دهند. خرابکاری کردن در یک وب سایت سطح بالا شبیه کشیدن ذغال گرافیک[2] بر روی یکی از بناهای یادبود ملی[3] است، به‌جز اینکه آن سایت برای کل دنیا وجود دارد تا با کلیک یک ماوس آنرا تماشا کنند. بسیاری از موارد هک شدن‌ها با پیام سیاسی، یا ضددولتی همراه بوده است.(۱۰۳)

هکرها تاکنون چندین وب سایت دولت آمریکا را مورد هدف قرار داده‌اند، از جمله اداره ملی فضا و هوانوردی[4]، وزارت دادگستری[5]، آژانس اطلاعات مرکزی[6]، نیروی هوایی[7] و وزارت کشاورزی[8]. در سال ۱۹۹۷ نوجوانی، وب سایت ناسا را هک کرد که در صفحات آن این عبارات خوانده می‌شد «ما صاحب شما هستیم، عجب وب درهم تنیده‌ای بافته‌ایم و تلاش می‌کنیم تا شما را فریب دهیم» و همچنین «مقامات دولتی که این سایت را اداره می‌کنند به‌شدت کودن هستند». صفحه مبدأ وزارت دادگستری جای خود را به صفحه‌ای داده بود که حاوی پس‌زمینه صلیب شکسته[9] و یک عکس رنگی از هیتلر که او را دادستان کل معرفی

---

1. Web Hacks
2. Graffiti
3. National Monument
4. National Aeronautics and Space Administration
5. Department of Justice
6. Central Intelligence Agency
7. Air Force
8. Department of Agriculture
9. Swastikas

می‌کرد، یک عکس بدون سر از یکی از ستارگان محبوب تلویزیون و اظهارات ضددولتی بود. عنوان این صفحه «وزارت بیدادگستری» شده بود. وب سایت هک شده سازمان مرکزی اطلاعات (سیا) همراه لینک‌هایی به عکس‌های برهنه با این جمله خوشامد می‌گفت که «به سازمان مرکزی حماقت» خوش آمدید.(۱۰۴)

در وب سایت نیروی هوایی نیز با یک عکس هرزه‌نگارانه[1]، فحش‌های رکیک و عبارات ضددولتی هک شده بود.(۱۰۵) خرابکاران در انگلستان صفحه مبدأ سایت «ملت اسلام»، «سازمان آمریکایی روان درمانی» و احزاب کارگر و محافظه‌کار را تغییر داده‌اند. هکرهای لهستانی هم صفحات وب تازه ایجاد شده هیأت وزیران خود را با صفحات دیگری تعویض می‌کردند.(۱۰۶)

در ماه مه سال ۱۹۹۷ بزرگ‌ترین شرکت سوئدی در زمینه بسته‌بندی گوشت به نام Scan متوجه شد که صفحه مبدأ سایت این شرکت جای خود را به صفحه‌ای داده که در آن آمده است: «سبزیجات کثیف را بایکوت کنید. گوشت بیشتری بخورید، لبخند بزنید و شاد باشید». این صفحه دارای عکس‌هایی از اندام‌های انسان و قسمت‌هایی از اجزای نهنگ‌ها و یک لینک به مرکز قانون حقوق حیوانات بود.(۱۰۷)

در ژوئن سال ۱۹۹۸ گروهی از هکرهای بین‌المللی که خود را Milworm می‌نامیدند، وب سایت مرکز تحقیقات اتمی "Bhabha" هندوستان (BARC) را هک کردند تا اعتراض خود را به آزمایش‌های اخیر سلاّح‌های هسته‌ای در هندوستان نشان دهند.(۱۰۸)

اکثر موارد هک شدن وب به شکلی گستاخانه بدیهی است. حمله‌ای آرام‌تر برای این منظور انجام می‌شود تا تغییراتی کوچک، اما مهم بر روی اسناد منتشر شده، داده شود تا اطلاعات غلط توزیع گردند. چندین روز طول می‌کشد تا اطلاعات اشتباه، شناسایی شوند. در این بین، بازدیدکنندگان از آن سایت، ممکن است براساس این اطلاعات غلط دست به اقدام زنند.(۱۰۹)

مرکز مطالعات جنگ‌های زیربنایی[2] اعلام کرد که ۴۷ مورد گزارش شده از حوادث مربوط

1. Pornographic Image
2. The Centre for Infrastructural Warfare Studies (CIWARS)

به هک‌شدن صفحات وب را از اول اوت تا ۱۵ اکتبر سال ۱۹۹۷ دریافت کرده‌اند و به این ترتیب ۲۱ مورد در ماه سپتامبر، ۱۴ مورد در ماه اوت و ۱۲ مورد در نیمه اول ماه اکتبر به ثبت رسیده است.[۱۱۰]

سایت‌های آمریکایی ۴۰ حمله، آلمانی ۲ حمله و سایت‌های کشورهای کانادا، نروژ، مالزی، ژاپن و اتریش هر کدام یک حمله را دریافت کرده‌اند. قربانیان، شامل مؤسسات دولتی آمریکا (۴)، شرکت‌ها (۳۱)، دانشگاه‌ها و کالج‌ها (۷) و سایت‌های سیاسی و رقیب (۵) بودند. این مرکز، متوجه شد که وب‌های هک شده «در مطبوعات مردمی گزارش نفس‌گیری دریافت می‌کنند، اما در حقیقت، خسارت بسیار اندکی از نظر سرقت و دستکاری داده‌ها به وقوع می‌پیوندد». در اواسط ماه دسامبر، آنها ۱۸ مورد Login را در عرض یک هفته گزارش دادند که دوباره اکثر موارد در آمریکا (۱۱) و انگلستان (۴) مورد داشت.[۱۱۱]

بنا بر اعلام سایت Hacked.net تعداد سایت‌های هک شده در ماه از ۳ مورد در ماه مارس ۱۹۹۷ (از زمانی‌که ثبت حوادث را آغاز کردند) به ۸۳ مورد در دسامبر سال ۱۹۹۷ افزایش پیدا کرد.[۱۱۲]

۱۳ـ۳ـ هک کردن سرویس نام قلمرو (domain name)

روش دیگر برای دستکاری آنچه تماشاگران در هنگام مراجعه به یک وب سایت می‌بینند، از طریق دستکاری در سرویس نام قلمرو (DSN) است به طوری‌که نام قلمرو سایت موردنظر تبدیل به آدرس IP سایت دیگری می‌شود. مثلاً اگر آدرس IP برای آدرس www.victim.com این باشد: ۳۳/ . ۲۲۲. ۷۷. ۶۶ بانک اطلاعاتی سرویس نام قلمرو را می‌توان طوری تغییر داد که نام قلمرو به آدرس IP یک سایت هرزه‌نگار لینک شود. کاربرانی که مرورگرهای خود را به طرف آدرس www.victim.com می‌گیرند، به سوی یک سایت پورنو هدایت شده و هیچ راهی برای به‌دست آوردن سایت درست نخواهند داشت، مگر اینکه آدرس IP آنرا با دست تایپ کنند.[۱۱۳]

یوجین کاشپورف[1]، مسئول مالی ارشد شرکت AlterNIC طوری سرویس قلمرو را هک کرده بود که کاربرانی که قصد داشتند وارد صفحه InterNIC شوند، از صفحه AlterNIC سر درمی‌آوردند.(۱۱۴)

در امری که ممکن است بزرگ‌ترین اشغال انبوه صفحات مبدأ باشد، هکرهای Milworm که ضدفعالیت‌های هسته‌ای هستند در حمله‌ای که بر روی بیش از ۳۰۰ وب سایت در ژوئیه سال ۱۹۹۸ تأثیر گذارد، به گروه هکرهای Ashtray Lumberjacks ملحق شدند.(۱۱۵) بنا بر گزارش‌های منتشر شده، این هکرها به شرکت انگلیسی ارائه‌دهنده خدمات اینترنتی به نام Easy Space که میزبان این سایت‌ها بود، حمله کرده بودند. آنها بانک اطلاعاتی این شرکت را طوری تغییر دادند که کاربران در حال تلاش برای دسترسی به این سایت‌ها به طرف یکی از سایت‌های MilwOrm هدایت شوند و در آنجا با پیام‌هایی که در اعتراض به مسابقه تسلیحات هسته‌ای بود به آنها خوشامد می‌گفتند.(۱۱۶) این پیام‌ها با این جمله به پایان می‌رسید: «از قدرت خود استفاده کنید تا دنیا را در حالت صلح حفظ کنید و به این گندکاری هسته‌ای پایان دهید». جان ورانسوویچ که سایت خبری هکری Anti Online را اداره می‌کند، گفت: «آنها معادل بمب‌گذار مرکز تجارت جهانی هستند. آنها می‌خواستند این قصه گفته شود تا توجه دیگران را به خود جلب کنند».(۱۱۷)

۱۴ـ۳ـ پیاده کردن[2]

بعضی از حملات با تأثیر انهدام داده‌ها[3] یا بروز وقفه در کارکرد[4] همراه هستند. این حملات به نام حملات «توقف خدمات»[5] معروف هستند زیرا کاربران قانونی، از سرویس و دسترسی به منابع اطلاعاتی محروم می‌شوند. در برخی موارد، خسارات گزارش شده هنگفت بوده است. در یک سخنرانی درباره تروریسم اطلاعاتی[6] خاطرنشان شد که یک شرکت تولیدی در سوئد بعد

---

1. Eugene Kashpureff
2. Take Down
3. Destroying Data
4. Disrupting Operation
5. Denial of Service
6. Information Terrorism

از حمله‌ای به شبکه‌های منطقه محلی آنان (LAN) دچار ۷ میلیون دلار خسارت شده است. گفته می‌شد که هزینه احیای سیستم ۲ میلیون دلار و هزینه رفع نقایص امنیتی ۵۰۰ هزار دلار است.(۱۱۸)

اقدامات خرابکارانه[1] بیشتر، کار کارمندان اخراجی است که در انتقام از دست دادن کار خود به کامپیوترهای کارفرمای سابق خود حمله می‌کنند.(۱۱۹)

با وجودی‌که اکثر هکرها، خسارت شدیدی بر سیستم‌هایی که مورد نفوذ قرار می‌دهند، ایجاد نمی‌کنند اما برخی این کار را انجام می‌دهند. مثلاً در دسامبر سال ۱۹۹۴ سیستم‌های کامپیوتری دانشکده نیروی دریایی آمریکا مورد حمله هکرهای ناشناخته‌ای قرار گرفت. این متجاوزان به ۲۴ سرویس‌دهنده دسترسی پیدا کردند و بر روی ۸ مورد از آنها، برنامه‌های Sniffer نصب کردند. آنها اسم و آدرس یک دستگاه را تغییر دادند و موجب شدند تا برای کاربران مجاز غیرقابل دسترسی شود. آنها یکی از فایل‌های پشتیبان سیستم را پاک کرده و فایل‌های موجود بر روی چهار سیستم دیگر را حذف کردند. همچنین این متجاوزان، شش سیستم دیگر را خراب کرده و ۱۲ هزار اسم رمز را نیز تغییر دادند.(۱۲۰)

در حادثه‌ای دیگر، متجاوزان به کامپیوترهای دانشگاه جورج میسون، فایل‌های بیش از ۴۰۰ دانشجو را در ژوئیه سال ۱۹۹۷ پاک کردند.(۱۲۱)

یکی از اقدامات خرابکارانه که شامل ایجاد حساب‌های کامپیوتری تقلبی[2] بود، در نهایت منجر به یک حمله محرومیت از خدمات برضد یک کاربر مجاز شد.(۱۲۲)

اکثر اقدامات خرابکارانه مانند، هک کردن صفحات وب ممکن است در حکم اعتراض به سیاست‌ها یا رویه‌های سازمان مورد حمله باشند.(۱۲۳)

گزارش‌های اندکی از حق‌السکوت سایبر[3] مطرح شده است. ساندی تایمز[4]، چاپ لندن در ۲۲ ژوئن سال ۱۹۹۶ مقاله‌ای را منتشر ساخت که در سرتیتر آن آمده بود: «شهر تسلیم تبهکاران

---

1. Sabotage
2. Creation of Phony Computer Accounts
3. Cyber Blackmail
4. Sunday Times

۴۰۰ میلیون دلاری شد». این مقاله اعلام کرده بود که مؤسسات آمریکایی و انگلیسی مجری قانون در حال بررسی ۴۰ حمله شناخته شده به مؤسسات مالی هستند که از سال ۱۹۹۳ در لندن و نیویورک به وقوع پیوسته است. این مقاله اعلام کرد که تروریست‌های سایبر، مشغول استفاده از ابزارهای پیشرفته جنگ اطلاعاتی هستند، از جمله بمب‌های منطقی[1] و تفنگ‌هایی با فرکانس رادیویی پرانرژی.[2] (۱۲۴)

۱۵ـ۳ـ از کار انداختن از راه دور[3]

خرابکاران با برخی از انواع حملات، می‌توانند از راه دور سرویس‌دهنده‌ای را از کار بیندازند، بدون اینکه وارد سیستم هدف شوند. در اغلب موارد، این امر شامل بمباران سرویس‌دهنده با بسته‌های طولانی یا تعداد زیادی از بسته‌هایی است که سرویس‌دهنده آماده سروسامان دادن به آنها نیست.(۱۲۵)

بعضی از سیستم‌ها را می‌توان با استفاده از برنامه ping (که حسن تعبیری برای «صدای جرینگ مرگ»[4] است) دچار وقفه نمود. معمولاً از این برنامه، برای تعیین این نکته استفاده می‌شود که آیا دستگاه دیگری در این شبکه فعال است یا خیر. فرستنده اقدام به فرستادن یک بسته ping از نوع «پروتکل کنترل پیام اینترنتی» به هدف می‌کند و هدف در صورتی‌که فعال باشد، پاسخ می‌دهد. جرینگ مرگ با ارسال بسته‌ای بلند، متشکل از ۶۵۵۳۶ بایت کار می‌کند (برعکس ۶۴ بایت پیش‌گزیده). با وجودی‌که این بسته بلند اعتبار ندارد، اما ایجاد یک بسته به‌علت استفاده از روش شکستن بسته‌ها برای راحتی کار ارسال، غیرممکن نیست. وقتی این قطعات شکسته شده دوباره در نزد گیرنده کنار هم نشانده می‌شوند، باعث سرریز شدن بافر شده که این خود اثرات جنبی متعددی دارد، مانند بوت مجدد یا از کار افتادن کامل. کمی پس

---

1. Logic Bombs
2. High-energy radio Frequency guns (HERF)
3. Remote Shutdown
4. Ping of Death

از اینکه نقطه ضعف اعلام شد شرکت‌های تولیدکننده شروع به صدور موارد رفع عیب این نقیصه امنیتی که بر روی پروتکل‌های شبکه تأثیر گذاشته است، می‌کنند.(۱۲۶)

حمله دیگری که از برنامه ping استفاده می‌کند به نام Smurfing معروف است. فرد مهاجم جریان بزرگی از بسته‌های ping را برای یک آدرس پخش می‌فرستد که خود یک آدرس IP است که در خدمت شبکه‌ای از کامپیوترهاست.(۱۲۷) تمامی بسته‌ها دارای آدرس مبدأ خاص خود و آدرس تقلیدی طرف قربانی هستند. تحت شرایط خاصی، میزبان پخش این بسته‌ها را به تمام میزبان‌های موجود بر روی شبکه خود رله می‌کند. این میزبان‌ها به نوبه خود به قربانی پاسخ داده و هر یک مقدار مساوی از داده‌ها را به کار خواهند برد. بنابراین، تأثیر آن این است که میزان داده‌های موجود با ضریبی معادل تعداد میزبان‌ها افزایش پیدا کند.(۱۲۸) مثلاً اگر مهاجم یک جریان ۷۶۸ کیلوبایت بر ثانیه‌ای از بسته‌های ping را به یک شبکه با ۱۰۰ میزبان ارسال کند، آن شبکه یک جریان ۷۶/۸ مگابیت در ثانیه تولید کرده و به قربانی بازمی‌گرداند و به این ترتیب نه تنها شبکه قربانی را مسدود می‌کند، بلکه شبکه، میزبان پخش را هم از کار می‌اندازد. ابزارهای اتوماتیک[1] به این افراد امکان می‌دهند تا به‌طور همزمان از چند میانجی استفاده کنند. می‌توان سیستم‌ها را طوری پیکره‌بندی نمود تا از مورد سوءاستفاده قرار گرفتن در این نوع حملات اجتناب شود. روش Smurfing به نام ping flooding یا حمله ICMP attack نیز معروف است.(۱۲۹) روش دیگر از کار انداختن سیستم بدون نفوذ به نام SYN flooding معروف است. در این حمله از همزمان‌سازی (synchronization) پروتکل کاربری شده برای آغاز یک ارتباط اینترنتی استفاده می‌شود. معمولاً این فرآیند با یک کامپیوتر آغاز می‌شود که بسته همزمان‌سازی (SYN) را به کامپیوتر دیگری (هدف) می‌فرستد.(۱۳۰) هدف با یک بسته SYN/ACK پاسخ می‌دهد که خود دریافت SYN را از طرف فرستنده اعلام می‌کند و با فرستادن یک SYN متعلق به خود به‌کار handshake ادامه می‌دهد. در نهایت، ارسال‌کننده یک بسته ACK پس می‌فرستد و SYN هدف را اعلام می‌کند. اکنون هر دو دستگاه آماده هستند تا داده‌ها را مبادله کنند.(۱۳۱)

---

1. Automatic tools

انواع دیگری از حمله از راه دور برای محروم ساختن از سرویس، شامل Teardrop، Bonk و UDP packet starm هستند. در روش Teardrop بسته‌هایی ناقص و معیوب فرستاده می‌شوند که حافظه را از حجم عظیمی از داده‌ها سرشار می‌کنند و منجر به از کار افتادگی دستگاه می‌گردند.(۱۳۲)

روش Bonk یکی از متغیرهای Teardrop است که کامپیوترهای دارای ویندوز ۹۵ یا N.T را از کار می‌اندازد. این روش، دستگاه را با بسته‌های معیوب[1] «پروتکل دیتاگرام کاربر»[2] (UDP) بمباران می‌کند. شرکت مایکروسافت به سرعت، یک patch را برای این روزنه امنیتی ارسال کرد، اما برای سایت سخنگوی Silicon Inverstor خیلی دیر شده بود. مدیران این سیستم با نومیدی شاهد این بودند که سرویس‌دهنده وب NT4.0 آنها به‌طور دائم دوباره بوت می‌شود. این حمله به مدت ۹/۵ ساعت ادامه یافت تا اینکه شرکت ارائه‌دهنده خدمات، شروع به فیلتر کردن بسته‌های UDP معیوب کرد. حمله‌ای از نوع UDP packet شامل لبریز کردن دستگاه با بسته‌های UDP می‌باشد.(۱۳۳) در یکی از این حملات، دو دستگاه به‌طور همزمان هدف گرفته می‌شوند و طوری تنظیم می‌گردند که یکدیگر را بمباران کنند. تأثیر حاصله ممکن است تراکم روی شبکه intertwining باشد به طوری‌که تمام میزبان‌های روی شبکه محروم از دسترسی شوند.(۱۳۴)

استیو بلووین و مات بلیز[3]، محققان امنیتی در شرکت AT&T هشدار دادند که خرابکارها می‌توانند جهت انجام حملات گسترده برای محروم کردن از خدمات، از نقاط ضعف موجود در طراحی اینترنت استفاده کنند.(۱۳۵) بلووین با ذکر رشته‌ای از حوادث که منجر به قطع خدمات، از دست رفتن نام قلمرو، یا مسیریابی مجدد ترافیک شد، می‌گوید: «من از کسی می‌ترسم که متوجه این حوادث شود و بگوید؛ آهای، من هم می‌توانم همین کار را انجام دهم». این محققان، خاطرنشان کردند که سیستم مسیریابی نامتمرکز، مسیر بسته‌های اطلاعات را از مبدأ تا مقصد پیدا می‌کند و

---

1. Corrupt
2. User Datagram Protocol
3. Steve Bellovin and Matt Blaze

سیستم نامگذاری قلمرو، به‌طرز خاصی آسیب‌پذیر است. خرابی تصادفی جدول‌های مسیریابی منجر به این شد که ترافیک دوباره از طریق دستگاه‌های کند مسیریابی شده یا در کل، مسدود شود و خرابی بانک اطلاعاتی به نام قلمرو «com.»[1] که باعث شد سایت‌های تجاری تا چندین ساعت غیرقابل دسترسی باشند.(۱۳۶) جاسوسان نیز می‌توانند این سیستم‌ها را مورد بهره‌برداری قرار دهند. بلووین می‌گوید: «زحمت هک کردن یک دستگاه را به خود ندهید تا در شبکه مشغول استراق‌سمع شوید. مسیر تمام ترافیک را به طرف دستگاه خود هدایت کنید».(۱۳۷)

برخی تلاش کرده‌اند تا وب سایت‌ها را با مسدود کردن از طریق ترافیک بیش از حد که کاربران دیگر نتوانند به آن دسترسی داشته باشند از کار بیندازند. گروهی که خود را Strano Networks می‌نامند این روش را به‌عنوان یکی از راه‌های اعتراض به سیاست‌های دولت فرانسه در زمینه مسائل هسته‌ای و اجتماعی امتحان کردند. این حمله در ۲۱ دسامبر سال ۱۹۹۵ برضد مؤسسات مختلف دولتی آغاز شد.(۱۳۸)

اگر وب سایتی برای نظرسنجی از بازدیدکنندگان دارای فرم‌هایی باشد، می‌توان آن سایت را با اسکریپت‌های رأی‌گیری اتوماتیک[2] از کار انداخت. در نوامبر سال ۱۹۹۷، روزنامه USA Today مجبور شد یک فرم نظرسنجی[3] را تعطیل کند، در این فرم از بازدیدکنندگان سایت درخواست می‌کرد تا آهنگ‌های دلخواه دوران کالج خود را رتبه‌بندی کنند، زیرا آنها از ترافیک حاصل از برنامه‌های رأی‌گیری مستأصل شده بودند. یکی از طرفداران اهل میشیگان در عرض ۶ ساعت ۶۰ هزار بار رأی داد.(۱۳۹)

۱۶ـ۳ـ حد نهایی[4]

حد نهایی[5] هک کردن در هیچ کشوری شناخته شده نیست. گزارش سازمان‌هایی که

1. Corruption of the ".com" Domain Name Database
2. Automated Voting Scripts
3. Survey asking
4 . Extent
5. The Total extent

تلاش‌های موفق و ناموفقی را برای نفوذ ردیابی می‌کنند، نشان می‌دهد که این حد قابل توجه است.

دیگر مطالعات نشان داده‌اند که موارد نفوذ در کامپیوتر فراگیر هستند و همچنان فراگیر خواهند ماند. داده‌های به‌دست آمده از نظرسنجی CSI/FBI نشان داد که درصد سازمان‌هایی که موارد نفوذ بیگانگان را گزارش کرده‌اند از ۱۸٪ در سال ۱۹۹۷ به ۲۱٪ در سال ۱۹۹۸ افزایش پیدا کرده[۱۴۰] و خسارت‌های گزارش شده در سال ۱۹۹۸ از ۵۰۰ دلار تا ۵۰۰ هزار دلار در نوسان بوده است. مجله Infosecurity News اعلام کرد که ۲۷ درصد پاسخ‌دهندگان به نظرسنجی[1] سال ۱۹۹۷ مواردی از تلاش برای دسترسی به سیستم‌های خود از طرف بیگانگان را گزارش کردند و ۸٪ اظهار داشتند که متجاوزان در کار خود موفق بوده‌اند.[۱۴۱] اداره پلیس ملی ژاپن گزارش‌هایی از ۹۴۶ مورد هک کردن را در ۶ ماه نخست سال ۱۹۹۷ دریافت کرد. این میزان به نسبت ۶ ماه نخست سال ۱۹۹۶، ۲۵٪ افزایش نشان می‌دهد.[۱۴۲] تیم واکنش اضطراری کامپیوترهای استرالیا[2] گزارش داد که حملات هکرها از سال ۱۹۹۶ تا ۱۹۹۷، ۲۲۰٪ افزایش داشته است.[۱۴۳]

---

1. Survey
2. The Australian Computer Emergency Response Team

فصل چهارم

۱ـ۴ـ حمله به قلب اینترنت

۲۱ اکتبر ۲۰۰۲، ساعت ۴ بعدازظهر به وقت شرق آمریکا، در حالیکه افکار عمومی خصوصاً در آمریکا در سرگردانی و وحشت اضافه شدن آخرین قتل تک تیرانداز آمریکایی به سر می‌بردند، خبر بر روی سایت اینترنتی Matrix Net System همچون بمبی بر خبرهای دیگر سایه انداخت. یک حمله اینترنتی از نوع Distributed Denial of Service که به اختصار به آن «DDOS» گفته می‌شود، توسط سیستم کنترل‌کننده این شرکت گزارش شده است. این حمله ۱۳ سرور اصلی اینترنت[1] را دربر می‌گیرد که وظیفه آنها کنترل آدرس‌های اینترنتی و ترجمه آن برای شبکه‌های DNS است. هر چند این خبر در هیاهوی دستگیری «جان‌آلن»، فردی که مظنون شماره یک قتل‌های زنجیره‌ای در آمریکا معرفی گشت، گم می‌شود، اما واقعیت این است که ارزش خبری آن در محیط مجازی اینترنت، همچون برخورد هواپیما به برج‌های مرکز تجارت جهانی در واقعیت است. این حمله حساب‌شده که به سرورهای اصلی اینترنت در سراسر جهان صورت گرفت در حقیقت نخستین و بزرگ‌ترین حمله در نوع خود بود که به اعتقاد بسیاری از کارشناسان در حافظه اینترنت چنین حمله‌ای مشاهده نشده است. سایت Matrix Net System که در حقیقت وظیفه مانیتور و مراقبت از ترافیک اینترنتی را برعهده دارد، ضمن اشاره به کاهش بار ترافیک در اثر این حمله، اسامی سرورهای مورد حمله

1. Internet Main Server

قرار گرفته را به ترتیب زیر اعلام کرد:

۱. Verisign ـ واقع در ویرجینیای آمریکا؛

۲. USDOD ـ واقع در ویرجینیای آمریکا؛

۳. لابراتوار تحقیقات ارتش ـ واقع در مریلند آمریکا؛

۴. Atonomica ـ استکهلم سوئد؛

۵. Reseaux IP Europeans ـ لندن انگلستان؛

۶. Wide Project ـ توکیو ژاپن.

چند ساعت پس از این، اعلام می‌شود که ۵ سرور مرکزی دیگر نیز مورد حمله قرار گرفته‌اند، یعنی از ۱۳ سرور مرکزی که به‌دلایل امنیت فیزیکی در سراسر جهان پراکنده‌اند همه بدون استثنا مورد حمله واقع شدند، آن هم درست در زمانی مشخص و از این میان ۹ سرور به‌طور کامل از کار می‌افتند، اما ۴ سرور باقیمانده در غیاب دیگر هسته‌های مرکزی اینترنت، کار انتقال ترافیک اینترنت[1] را برعهده می‌گیرند.

واقعه آنقدر بزرگ است که «آری فلیشر»، سخنگوی کاخ سفید با تمام سعی و تلاشی که در خونسرد نشان دادن خود به‌کار می‌برد، کمی می‌لرزد. او می‌گوید: «مشخص نیست که این حمله از کجا سرچشمه می‌گیرد هرچند ممکن است در نهایت مشخص شود که این حمله یک کار تروریستی مجازی Cyber Terrorism باشد. سابقه تاریخی نشان می‌دهد که این‌گونه حمله‌ها معمولاً توسط گروه‌های نفوذگر (هکر) سازماندهی می‌شوند، البته مأموران ما در حال تحقیقاتی هستند».

اما با سخنان فلیشر کار به پایان نمی‌رسد. بوش نیز کمی بعد در سخنرانی خود درباره محافظت کودکان در برابر خطرات اینترنتی به این حمله اشاره می‌کند و آنرا یک نوع تروریسم اینترنتی می‌نامد. درست یک روز پس از این حادثه FBI اعلام می‌کند که هرچند تأثیر این

1. Traffic in Internet

حمله بر روی کاربران معمولی اینترنت[1] ناچیز بوده، اما حمله بزرگ‌ترین تلاش برای از کار انداختن اینترنت (و نه فقط چند سایت) از ابتدای پیدایش آن بوده است. نکته جالب در این ماجرا، جنگ پنهان مدافعان سرور با مهاجمان در زمان حمله بود. پل ویکسی از کمپانی Consor Tium Internet Software می‌گوید: «اگر سرورها تنها کمی بیشتر خاموش می‌ماندند و اگر هکرها تنها موفق به حفظ موقعیت خود در خاموش نگاه داشتن سرورها می‌شدند، در آن صورت هیچ کاربری به اینترنت متصل نبود و در نتیجه همه درگیر یک فاجعه بزرگ بودیم».

اما شاید چنین اتفاقی لازم بود تا طراحی دقیق شبکه بزرگی که همه آنرا اینترنت می‌نامند، مشخص شود. کریس مارو، متخصص امنیت شبکه VUNET می‌گوید: این احتمالاً بزرگ‌ترین حمله همه‌جانبه و هماهنگ به ساختار اینترنت بود، اما VUNET که دو سرور از ۱۳ سرور اصلی را در اختیار دارد، توانست در غیاب سرورهای خاموش دیگر ترافیک اینترنت را کنترل کند. این موضوع نشان‌دهنده ساختار کامل و بی‌عیب اینترنت است. به گفته پل ویکسی، تنها ۴ یا ۵ سرور در مقابل حمله اخیر مقاومت کردند. در حقیقت هکرها با برنامه‌ریزی مشخص، قصد خاموش کردن اینترنت را داشتند و اگر مقاومت یکی دو سرور و انتقال ترافیک به آنها نبود، اکنون وضعیت کاملاً بحرانی بود.

اما چگونه این چند سرور در مقابل چنین حمله‌ای مقاومت کردند. پل ویکسی که سرور شرکت او در مقابل حمله، ضربه نخورده بود، می‌گوید: «ما انتظار چنین چیزی را داشتیم و در حقیقت Verisign کاملاً آماده بود». به گفته کارشناسان، هکرها خوب می‌دانستند که چه می‌خواهند. آنها از روش ساده و پیش پا افتاده‌ای برای حمله استفاده کردند، اما به‌دلیل حجم زیاد و حمله هماهنگ کار آنها مانند یک موج بزرگ درآمد. هکرها قصد داشتند، سیستم نام دامنه یا Domain Name اینترنت را از کار بیندازند. این سیستم وظیفه برگرداندن یا ترجمه کدهای آدرس پروتکل اینترنت به لغات معمولی[2] را دارد. در حقیقت، زمانی‌که این سیستم از کار بیفتد حتی در صورت

---

1. Usually Users
2. Usually Words

وجود ارتباط اینترنتی، دستورهای کاربران به هدر رفته و در هیاهوی دستورهای نامشخص در اینترنت گم خواهد شد.

اما از طرف دیگر، هکرها چنین شانسی را برای از کار انداختن اینترنت حداقل در کوتاه‌مدت از دست دادند. چراکه با این حمله توجه متخصصان امنیت شبکه بر روی این بخش اینترنت کاملاً متمرکز شده است. مهندسان اینترنتی بسیار سریع با برطرف کردن ضعف سرورهای خود، راه‌های نفوذ از این طریق را بستند، اما در این میان هکرها هم بیکار نخواهند نشست، آنها نیز با بررسی شکست خود در این حمله، راه‌های دیگری را خواهند آزمود.

تحقیقات در مورد یافتن عوامل حمله‌کننده این واقعه از نخستین ساعات حمله آغاز شد. پلیس FBI یک دایره ویژه برای رسیدگی به چنین جرم‌هایی در اختیار دارد.(۱۴۴)

۲ـ۴ـ آسیب‌پذیری آمریکا

کشور آمریکا به‌شدت به سیستم‌های رایانه‌ای وابسته است. در پی حملات تروریستی ۱۱ سپتامبر علیه این کشور، دولت آمریکا تدابیر امنیتی در اینترنت را تشدید کرده است.

جورج بوش، رئیس‌جمهور آمریکا، دستور داد ۱/۵ میلیارد دلار بر بودجه تدابیر امنیتی شبکه‌های رایانه‌ای و اینترنت و همچنین آموزش متخصصانی که با حملات اینترنتی احتمالی تروریست‌ها مقابله می‌کنند، افزوده شود.

آقای نایتس گفت: «نکته تناقض‌آمیز این است که آمریکایی‌ها از لحاظ به راه انداختن نبرد اطلاعاتی در جهان نظیری ندارند، همچنین آمریکا بیش از سایر کشورها در مقابل حملات اینترنتی آسیب‌پذیر است».

در مورد احتمال وقوع چنین حمله‌ای آرای گوناگونی ابراز می‌شود. برخی ناظران به سناریویی احتمالی اشاره می‌کنند که در آن حمله‌ای الکترونیکی[1] باعث ایجاد اختلال گسترده در شبکه برق‌رسانی و سیستم‌های ارتباطی و مالی خواهد شد.

---

1. Electronic Attack

آقای نایتس هم گمان نمی‌کند که عراق بازیگری جدی در هرگونه نبرد اینترنتی باشد. اما شرکت «ام آی ۲ جی» این تهدید را جدی‌تر قلمداد می‌کند.

آقای ماتای گفت: «ویروس اسلمر (Slammer) کره را فلج کرد، ۱۳ هزار دستگاه عابر بانک[1] در آمریکا را از کار انداخت و خدمات اضطراری در شهر سیاتل را مختل نمود».

او سناریویی را تجسم می‌کند که در آن قطعه‌ای از یک نرم‌افزار مخرب در شبکه‌های رایانه‌ای منتشر می‌شود و در اینترنت اختلالات جدی به‌وجود می‌آورد. به گفته وی چنین حمله‌ای تنها با حمایت‌های دولتی ممکن است.[۱۲۵]

۳ـ۴ـ هراس از حملات اینترنتی القاعده

گفته می‌شود مقامات ایالات‌متحده در حال بررسی تهدیدات اینترنتی هستند که ممکن است سازمان القاعده برای این کشور ایجاد کند. تحقیقات در این زمینه براساس آخرین اطلاعات و شواهد در مورد تلاش برای نفوذ به سیستم‌های الکترونیکی آمریکا از کشورهای خاورمیانه و جنوب آسیا انجام می‌شود.

تا این اواخر، مقامات آمریکایی تنها متوجه تهدیدات اینترنتی هماهنگ‌شده از سوی عوامل دولت‌هایی چون چین و روسیه بودند. این مقامات پیش‌تر بر این عقیده بودند که القاعده تمایل و قابلیت‌های کمی برای انجام حملات الکترونیکی جدی دارد.

مراقبت‌های اینترنتی

براساس گزارش روزنامه واشنگتن پست، در پاییز سال گذشته مقامات محلی، دفتر تحقیقات فدرال (FBI) و آزمایشگاه ملی «لارنس لیورمور»، مشغول بررسی شیوه مشکوک زیر نظر گرفتن رایانه‌های «دره سیلیکون»[2]، محل استقرار صنایع

---

1. ATM

2. Silicon Valley

الکترونیکی آمریکا، بودند. خلاصه‌ای از این بررسی، که توسط وزارت دفاع ایالات‌متحده تهیه شده، چندین مورد حمله به سایت‌های مستقر در کالیفرنیا و سایر نقاط آمریکا را گزارش کرده است.

این نظارت، از طریق سیستم‌های مخابراتی عربستان‌سعودی، اندونزی و پاکستان انجام گرفت و بر روی سیستم‌های اورژانس تلفنی، منابع، توزیع آب و شبکه و نیروگاه‌های قدرت متمرکز بود.

اطلاعات بیشتر در مورد چنین سیستم‌هایی، در رایانه‌های کشف و ضبط شده از القاعده در حملات افغانستان، نیز به‌دست آمد.

سیستم‌های کنترل

بازجویی از عاملان دستگیر شده القاعده نشان داد که این «گروه تروریستی» به‌نوع خاصی از دستگاه‌های دیجیتال علاقه‌مند بودند که در سیستم‌های کنترل توزیع شده[1] و سیستم‌های کنترل نظارت و جمع‌آوری داده‌ها (SCADA) به‌کار می‌رود.

از سیستم‌های کنترل توزیع شده در ۲۰ سال گذشته در راه‌اندازی واحدهای صنعتی، شامل پالایشگاه‌های نفت و نیروگاه‌های برق استفاده شده است. سیستم‌های کنترل نظارت و جمع‌آوری داده‌ها، فناوری جدیدتری می‌باشد.

اندرو باند، سردبیر یک نشریه در مورد اتوماسیون صنعتی می‌گوید: «این دستگاه‌ها در کنترل عملیات صنعتی به‌کار می‌روند و اخیراً در سیستم‌های تجاری مرتبط به اینترنت هم استفاده می‌شوند».

FBI در اوایل سال هشدار داده بود که عوامل القاعده در حال بررسی سیستم‌های کنترل و جمع‌آوری داده‌ها هستند و کاربرد این دستگاه‌ها را در سیستم آبرسانی و مدیریت فاضلاب بررسی می‌کنند.

---

1. Distribution Control Systems (DCS)

بررسی احتمالات

ریچارد کلارک، رئیس امنیت سیستم‌های اینترنتی آمریکا، یکی از افرادی است که از مدت‌ها پیش در مورد یک حمله غافلگیرکننده بر روی زیرساخت عظیم دیجیتال ایالات‌متحده، موسوم به «پرل هاربر دیجیتال»، هشدار داده است.

در گذشته، برخی از کارشناسان امور ایمنی چنین اظهاراتی را رد کرده و می‌گفتند که کنترل سیستم‌های صنعتی و خدماتی، مانند کنترل ترافیک هوایی، نیروگاه‌های برق، منابع آب و خدمات بهداشتی و اورژانس، از اینترنت جداست. اما اندرو باند می‌گوید که راه‌هایی برای دسترسی به چنین سیستم‌هایی از خارج وجود دارد.

اگرچه بسیاری از سیستم‌ها، مستقیماً به اینترنت متصل نیست، اما غالباً به سیستم‌های تجاری متصل‌اند که ممکن است به اینترنت وصل باشد. او می‌گوید، تهدیدهای جدی‌تر از حوادث عظیمی سرچشمه می‌گیرد که خارج از تصور کارشناسان است، مانند انجام یک حمله فیزیکی همزمان با نفوذ به سیستم‌ها.[۱۴۶]

پی‌نوشت‌ها

۱. خبرگـــزاری دانـــشجویان ایـــران، ایـــسنا، ۱۳۸۲/۱/۲۲، ســـرویس فنـــاوری اطلاعـــات
www.isna.ir/new

۲. رادیو آمریکا، شنود رادیویی ویژه این تحقیـق، مـورخ ۱۳۸۲/۲/۵، همچنـین ســایت فارسـی رادیو آمریکا،
www.VOAnews.com/persian

۳. بخش فارسی رادیو بی‌بی‌سی، ۱۳۸۲/۳/۱۱، www.bbc.co.uk/persian

۴. همان

5. The Asian wall street Journal

۶. همان

۷. رادیو مسکو، شنود رادیویی ویژه این تحقیق، مورخ ۱۳۸۲/۱/۳۰

8. Kevin Whitelaw, "Terrorists on the Web: Electronic 'Safe Haven,'" U.S. *News & World Report,* June 22, 1998, p. 46. The State Department's list of terrorist organizations is at http://www.state.gov/www/global/terrorism/index.html.

9. Robert Harkins, "Information Terrorism: A Trans-State Security Threat?" term project for COSC 511, Georgetown University, July 1997, citing L. Clarke, "IRA Uses Hi-Tech International Intelligence Bank," *Sunday Times,* London, Mar 9, 1997.

10. Statement of Louis J. Freeh, director of the Federal Bureau of Investigation, before the Committee on Commerce, Science, and Transportation, United States Senate, regarding the Impact of Encryption on Law Enforcement and Public Safety, Mar 19, 1997.

11. Matthew J. Littleton, "Information Age Terrorism," Master's thesis, Naval Postgraduate School, Dec 1995, pp. 75-76, citing John Lamb and James Etheridge, "DP: The Target of Terror," *Datamation, Vol.* 32, Feb 1, 1986.

12. Matt G. Devost, Brian K. Houghton, and Neal Allen Pollard, "Information Terrorism: Political Violence in the Information Age," 1996.

13. "E-Mail Attack on Sri Lanka Computers," *Computer Security Alert,* No. 183, Computer Security Institute, June 1998, p. 8.
14. Jim Wolf, "First 'Terrorist' Cyber-Attack Reported by U.S.," *Reuters,* May 5, 1998.
15. *CIWARS Intelligence Report,* May 10, 1998.
16. Barry Colin, "The Future of Cyberterrorism," *Crime and Justice International,* Mar 1997, pp. 15-18.
17. Mark M. Pollitt, "Cyberterrorism-Fact or Fancy?" *Proceedings of the 20th National Information Systems Security Conference,* Oct 1997, pp. 285-289.
18. *Computers at Risk,* National Academy Press, 1991.
19. Barry Colin, "The Future of Cyberterrorism," *Crime and Justice International,* Mar 1997, pp. 15-18.
20. Mark M. Pollitt, "Cyberterrorism-Fact or Fancy?" *Proceedings of the 20th National Information Systems Security Conference,* Oct 1997, pp. 285-289.
21. Tom Manzi, "Financial Warfare: Assessing Threats to the U.S. Financial Infrastructure," thesis for the Master of Science of Strategic Intelligence, Joint Military Intelligence College, Dec 1996.
22. Edward Browne, "Information Warfare and Finance: A Strategic Target," http://www.infowar.com.
23. Brad S. Bigelow, "The MacGuffin of Financial Information Warfare," *Journal of Infrastructural Warfare,* Summer 1997.
24. "Satellite Outage Continues as Paging Firms Scramble," *Wall Street Jounal,* May 21, 1998; Andrew Cain and Suzin Schneider, "Satellite Failure Renders Most Pagers Silent," *Washington Times,* May 21, 1998; *Associated Press,* May 22, 1998; Janet Kornblum, "Net Replaces Satellite for NPR," *CNET News,* May 20, 1998.
25. William Church, "Information Warfare Threat Analysis for the United States of America, Part Two: How Many Terrorists Fit on a Computer Keyboard?" *Journal of Infrastructural Warfare,* Summer 1997.
26. William Church, "Information Warfare: Threat Analysis," *Journal of Infrastructural Warfare,* Summer 1997.
27. Clark L. Staten, testimony before the Subcommittee on Technology, Terrorism and Government Information, U.S. Senate Judiciary Committee, Feb 24, 1998.
28. An excellent resource on the use of weapons of mass destruction in terrorism is James K. Campbell, *Weapons of Mass Destruction Terrorism,* Interpact Press, 1997.
29. John Markoff, "Airports Told of Flaw in Security System," *New York Times,* Feb 8, 1998.
30. John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy,* Vol. 12, 1993, pp. 141-165, in John Arquilla and David Ronfeldt, eds., *In Athenas Camp,* RAND, 1997, pp. 23-60. For an extended treatment, see John Arquilla and David Ronfeldt, "The Advent of Netwar," National Defense Research Institute, RAND, 1996.
31. David Ronfeldt and Armando Martinez, "A Comment on the Zapatista 'Netwar,'" in John Arquilla and David Ronfeldt, eds., *In Athena's Camp,* RAND, 1997, pp. 369-391.

32. "Communications posted at the Electronic Disturbance Theater Web site, http://www.nyu.edu/proiects/wray.
33. "Pentagon Beats Back Internet Attack," *Wired News*, Sep 10, 1998.
35. Marianne Swanson, "Introduction to FedCIRC," presentation. Information from FedCIRC is available at http://csrc.nist.gov/fedcirc.
36. Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, Oct 1997, Report Summary, http://www.pccip.gov.
37. Ibid.
38. *CIWARS Intelligence Report*, Centre for Infrastructural Warfare Studies, Jun 21, 1998; "Pentagon Computer Systems Hacked," *Info Security News*, Jun 1998; Douglas Pasternak and Bruce B. Auster, "Terrorism at the Touch of a Keyboard," *U.S. News & World Report, July* 13, 1998, p. 37.

۳۹. آدرس سایت اینترنتی فارسی وزارت امور خارجه آمریکا

40. www.jihadunspan.com

۴۱. سایت آی.تی ایران به نقل از نیویورک تایمز www.itiran.com/news

۴۲. این پرستار قلابی، دختر سفیر کویت در واشنگتن بوده و شهادت دروغین او توسط مایکل. کـا. دیور مشاور تبلیغاتی ریگان برای کابینه Rendon Group تهیه و تنظیم شده بود.

43. http://www.itiran.com/artic/show_user_archive.as?des=8105&id=23
44. http://www.itiran.com/artic/show_user_archive.asp?des=8204&id=70
45. Michael Stutz, "AOL: A Cracker's Paradise?" *Wired News*, Jan 29, 1998.
46. Jared Sandberg, "Hackers Prey on AOL Users with Array of Dirty Tricks," *Wall Street Journal*, Jan 5, 1998; Da Chronic, "AOHell v 3.0 Rage against the Machine," http:l/www.wco.con/~destiny/chronic2.htm.
47. David S. Hilzenrath, "Yale Student Pleads Guilty to Computer Fraud on AOL," *Washington Post*, January 9, 1997; "Hacker Sentenced for America Online Fraud," *Newsbytes*, Apr 1, 1997.
48. Mich Kabay, "Flashes from the Past," *Information Security*, Dec 1997, p.17.
49. Cliff Stoll, *The Cuckoo's Ego*, Po-ket Books, 1989, pp. 109-110.
50. Ibid., pp. 194-196.
51. Ibid., p. 328.
52. For example, see http://www.rootshell.com or http://www.geek-girl.com / bugtraq/.
53. *Information Week*, Apr 24, 1995, p. 22, as reported in *Edupage*.
54. Dan Farmer, "Shall We Dust Moscow? (a Semi-Statistical) Survey of Key Internet Hosts & Various Semi-Relevant Reflections," http://www.trouble.org/survey/, Dec 18, 1996.
55. E. Eugene Schultz and Thomas A. Longstaff, "Internet Sniffer Attacks," *Proceedings 18th National Information Systems Security Conference*, National Institute of Standards and Technology and National Computer Security Center,

Baltimore, MD, Oct 10-13, 1995, pp. 534-542. Reprinted in Dorothy E. Denning and Peter J. Denning, eds., *Internet Besieged: Countering Cyberspace Scofflaws,* ACM Press, 1997.

56. CERT Coordination Center 1996 Annual Report (Summary).
57. Jim Christy, "Rome Laboratory Attacks, Prepared Testimony before the Senate Governmental Affairs Committee Permanent Investigations Subcommittee," May 22, 1996. In Denning and Denning, *Internet Besieged.*
58. FedCIRC Incident Handling and Information Sharing, http://fedcirc.llnl.gov.

۵۹. روزنامه جام‌جم، شماره ۸۴۷، مورخ ۱۳۸۲/۲/۶، ص ۱۲.

60. http://www.itiran.com/artic/show_user_archive.asp?des=8106&id=56
61. http://www.itiran.com/artic/show_user_archive.asp?des=8104&id=16

۶۲. همان، ۱۳۸۱/۱۴/۱۴

63. Peter J. Denning, "The Internet Worm," and Eugene H. Spafford, "Crisis and Aftermah," in Peter J. Denning, ed., *Computers under Attack: Intruders, Worms, and Viruses,* ACM Press, Addison-Wesley, 1990.
64. Dan Farmer and Wietse Venema, "Improving the Security of Your Site by Breaking into It," 1993, http://www.trouble.org/security.
65. *Edupage,* Nov 1995, citing *Computerworld,* Nov 13, 1995, p.1.
66. Richard Behar, "Who's Reading Your E-Mail," *Fortune,* Feb 3, 1997.
67. http://www.10pht.com/10phtcrack; Ben Heskett, "A New Windows Password Cracker," *CNET,* Feb 13, 1998.
68. Adapted from William R. Cheswick and Steven M. Bellovin, *Firewalls and Internet Security,* Addison-Wesley, 1994, p. 39.
69. Dan Farmer and Wietse Venema, "Improving the Security of Your Site by Breaking into It," 1993, http://www.trouble.org/security.
70. Mark W. Loveless, "Misconfigured Web Servers," best-of-security list, Dec 26, 1995.
71. Mark Abene, posting to comp. security. unix, July 7, 1997.
72. CERT Coordination Center 1996 Annual Report (Summary), http://www.cert.org.
73. Nick Wingfield, "Newest MS Server Not Secure," *CNET,* Feb 20, 1997.
74. Ray Cromwell, messages posted to sci.crypt and alt.security, Sep 26, 1996. For a detailed explanation of buffer overflow bugs, see Aleph One, "Smashing the Stack for Fun and Profit," http://www.geek-girl.com /bugtraq/1996_4/0195.html.
75. Because the information provided by finger can be helpful to hackers, many sites, including Georgetown University, do not run fingerd.
76. "Buffer Overrun Vulnerability in statd(1M) Program," *CERT Advisory CA97.26,* Dec 5, 1997.
77. Bradley Graham, "11 U.S. Military Computer Systems Breached by Hackers This Month," *Washington Post,* Feb 26, 1998.
78. Rajiv Chandrasakaran and Elizabeth Corcoran, "Two California Teens Suspected of Breaking into Government Computers," *Washington Post,* Feb 28, 1998.

79. Steve Bellovin, "Network and Internet Security," in Dorothy E. Denning and Peter J. Denning, eds., *Internet Besieged: Countering Cyberspace Scofflaws,* ACM Press, Addison-Wesley, 1997.

80. Roger Dennis, "Internet Hacking Tool Threatens Web Users with Windows-Family Network," *South China Morning Post,* July 21, 1998.

82. Ira Winkler, *Corporate Espionage,* Prima, 1997, p. 94.

83. Ibid.

84. Ibid., p. 95.

85. Katie Hafner and John Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier,* Simon & Schuster, 1991, p. 60.

86. Jim Hu, "AOL Security Lapse Opens Accounts," *CNET,* May 28, "1998.

87. Jared Sandberg, "Hackers Prey on AOL Users with Array of Dirty Tricks," Wall *Street Journal,* Jan 5, 998; Da Chronic, "AOHell v 3.0 Rage against the Machine," http://www.wco.com/~destiny/chronic2.htm.

88. Jared Sandberg, "Hackers Prey on AOL Users with Array of Dirty Tricks," *Wall Street Journal,* Jan 5, 1998.

89. Jim Christy, Rome Laboratory Attacks, Prepared Testimony before the Senate Governmental Affairs Committee Permanent Investigations Subcommittee, May 22, 1996. In Denning and Denning, *Internet Besieged.*

90. Ibid.

91. Kristi Essick, "U.S. Navy Caught Hacking into British Marine Charity Web Site," *Info World Electric,* May 8, 1998.

92. Richard Thieme, "An Interview with Se7en" and "Se7en: The Sequel," *Computer Underground Digest,* Vol. 9, No. 49, Jun 24, 1997.

93. Dorothy E. Denning, *"The United States vs. Craig Neidorf," Communications of the ACM,* Vol. 34, No. 3, Mar 1991, pp. 24-32. The article is followed by a debate on electronic publishing, constitutional rights, and hacking.

94. Suelette Dreyfus, *Underground,* Mandarin, Australia, 1997, p. 196.

95. Patrick Townson, "Chicago Phreak Gets Prison Term," Feb 17, 1989.

96. Joshua Quittner, "Hacker Homecoming," *Time,* Jan 23, 1995.

97. Peter G. Neumann, *Computer Related Risks,* ACM Press, 1995, p. 154.

98. "Hacker Changes His Brother's Grades," *Computer Fraud & Security,* July 1997, p. 2.

99. Peter G. Neumann, *Computer Related Risks,* ACM Press, 1995, p. 176.

100. *Associated Press,* New York, Oct 24, 1997.

101. "The InfoSec Year in Review," *NCSA News,* Jan 1997, p. 6.

102. "FBI Helping Thailand to Catch Computer Criminals," *Newsbytes,* Bangkok, Thailand, Apr 14, 1998.

103. Many of the spoofed Web pages can be seen on the *2600 Web* site at http://www.2600.com.

104. John O'Neil, "Hacker Vandalizes Web Site of U.S. Justice Department," *New York Times,* Aug 18, 1997.

105. *Edupage,* Dec 31, 1996, citing *New York Times,* Dec 31, 1996, p. A9.

106. Linda McCarthy, *Intranet Security,* Sun Microsystems Press, Prentice Hall, 1997, p. 50.
107. Sylvia Dennis, "Polish Government Web Site Hacked-Police Investigate," *Newsbytes,* May 9, 1997.
108. Hackers Return to Wreak Havoc on Government Website," Central/Eastern Europe Polish News Bulletin of British & American Embassies, Jul 25, 1997.
109. James Glave, "Crackers: We Stole Nuke Data," *Wired News,* Jun 3, 1998; Janelle Carter, "Hackers Hit U.S. Military Computers," *Associated Press,* Washington, Jun 6, 1998; "Hackers Now Setting Their Sights on Pakistan," *Newsbytes,* June 5, 1998.
110. "Indian Nuclear Center Admits Hacker Break-in," *Newsbytes,* Tokyo, Japan, June 4, 1998.
111. *CIWARS Intelligence Report, Vol.* 1, Issue 8, Oct 19, 1997; http://www.iwar.org.
112. "Hacks of Public Pages Are Growing with the Internet," *Tasty Bits from the Technology Front,* Dec 24, 1997.
113. Michael Stutz, "Canadian Cops Keep Kashpureff Caged," *Wired News, Nov* 11, 1997.
114. United States District Court of the Eastern District of New York against Eugene E. Kashpureff, Defendant, complaint filed by Thomas H. Swink, Special Agent, Federal Bureau of Investigation, Sep 12, 1997.
115. Michael Stutz, "Canadian Cops Keep Kashpureff Caged," *Wired News,* Nov 11, 1997.
116. "AlterNIC Founder Extradited to U.S.," *Edupage,* Dec 21, 1997, citing *Net Insider,* Dec 18, 1997.
117. Jim Hu, "Political Hackers Hit 300 Sites," *CNET,* Jul 6, 1998. The Milw0rm page is shown at http://www.antionline.com.
118. Paul Strassmann, Information Terrorism, second of three lectures, Information Warfare Seminar, U.S. Military Academy, West Point, Oct 5, 1995.
119. *San Francisco Chronicle,* Jul 2, 1992; Jamie S. Gorelick, "Protecting Critical National Infrastructures Against the New Cyber Threat," in James P. McCarthy, ed., *National Security in the Information Age,* Conference Report, US Air Force Academy, Colorado Springs, CO, Feb 28 -Mar 1, 1996, p.153.
120. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, United States General Accounting Office, Report to Congressional Requesters, GAO/AIMD-96-84, May 1996, p. 25.
121. Ann O'Hanlon, "Hacker's Breach GMU Computers, Zap Student's Work,' *Washington Post,* Aug 8, 1997, p. B1. Peter Denning provided additional information.
122. Private conversation with Jonathan Littman on Jan 14, 1998; Joshua Quittner, "The Hacker's Revenge," *Time,* May 12, 1997.
123. Da Chronic, "AOHell v 3.0 Rage against the Machine," http://www.wco. com /~destiny/chronic2.htm.
124. Mark Glaser, "AOL 'Hacker Riot' More Like Amateur Hour," *Wired News,* Feb

17, 1997; Janet Kornblum, "AOL 'Riot' Falls Short," *CNET*, Feb 14, 1997.

125. Todd Fast, "CyberJihad, the Microsoft IIS Bug," http://www.eden.com/~tfast/jihad.html; http://www.microsoft.com/iis/iisnews/hotnews/issue tb.htm.

126. *Chronicle of Higher Education*, Nov 22, 1996, p. A23; It's the Ping o' Death Page!, http://prospect.epresence.com /ping/.

127. Craig A. Huegen, "The Latest in Denial of Service Attacks: 'Smurfing,' Description and information to Minimize Effects," Oct 18, 1997, http://www.quadrunner.com/~chuegen /smurf.txt; *CERT Advisory*, CA-98.01. smurf, Jan 5, 1998.

128. ProWatch Secure Network Security Survey (May-Sep 1997).

129. *Associated Press*, 1996.

130. Elizabeth Weise, "Computer Attack against WebCom," *Associated Press*, Dec 17, 1996.

131. Annaliza Savage, "TCP Bug Threatens Networked Computers," *Wired News*, Nove 21, 1997.

132. Rutrell Yasin, "Land and Teardrop Protection," *CMPnet*, Issue 693, Dec 8, 1997.

133. Michael Stutz, "Bonk! A New Windows Security Hole," *Wired News*, Jan 9, 1998.

134. "Microsoft's 'Bonk' Patch Too Late for Some," *Wired News*, Jan 13, 1998.

135. *CERT Advisory*, CA-96.01, Feb 8, 1996.

136. John Borland, "Want to Break the Net," *Tech Web*, Feb 20, 1998.

137. Information provided to the author from Bruce Sterling; Winn Schwartau, *Information Warfare*, 2nd ed., Thunder's Mouth Press, 1996, p. 407.

138. "How to Flood the White House," http://www.nyu.edu/projects/wray/May10how.html.

139. Adam Elman, "College Web Surveys Hazardous to Your Server's Health," *Risks-Forum Digest, Vol.* 19, Issue 46, Nov 17, 1997, citing http://www.usatoday.com/form/colsong.htm.

140. 1997 CSI /FBI Computer Crime and Security Survey, *Computer Security Issues & Trends*, Vol. III, No. 2, Spring 1997; 1998 CSI /FBI Computer Crime and Security Survey, *Computer Security Issues & Trends*, Vol. IV, No. 1, Winter 1998.

141. David S. Bernstein, *Infosecurity News* Industry Survey, *Infosecurity News*, May 1997, pp. 20-27.

142. CITE Report, Tracking Number: 4981997, Sep 10, 1997, http://www.iwar.org, .citing Martyn Williams, "Japan's Police Propose Anti-Hacker Guidelines," *Newsbytes*, Sept 5, 1997.

143. Beverley Head, "Computers-Network Security a Low Priority," *Australian Financial Review*, Dec 31, 1997, p. 14.

۱۴۴. شهرام شریف، بخش مقاله سایت itiran، ۸ آبان ۱۳۸۱.

www.itiran.com

145. http://www.itiran.com/artic/show_user_archive.asp?des=8111&id=17

146. http://www.itiran.com/index2.asp?1oc=/artic/show.asp?no=22 http://www.itiran.com/artic/show_user_archive.asp?des=8104&id=10

بخش دوم

تکنیک‌های جنگ رایانه‌ای

فصل اول

۱ـ۱ـ گرفتن سیگنال‌ها

محیط‌زیست به‌طور دائم مملو از انرژی‌های مغناطیسی و الکتریکی[1] شده است. این همان چیزی است که به ما امکان می‌دهد تا هر چیزی را در اطراف خود ببینیم و بشنویم. این انرژی به پزشکان امکان می‌دهد تا درون بدن را مشاهده کنند و خلبانان در هنگام شب از میان طوفان به پرواز درآیند، به نیروهای پلیس امکان می‌دهد، بدانند که ما در چه زمانی با سرعت، مشغول رانندگی هستیم و موشک‌ها را به طرف اهدافشان هدایت می‌کند. انرژی الکترومغناطیسی[2] حامل تمام پیام‌های مخابراتی ماست؛ از تماس‌های تلفنی گرفته تا فاکس‌ها و ترافیک شبکه کامپیوتری، این انرژی، برنامه‌های تلویزیونی را که تماشا می‌کنیم و ایستگاه‌های رادیویی را که گوش می‌کنیم، انتقال ی‌دهد. در میانه جلسات با سیستم پیجر (Pager) ما را پیدا می‌کند و به ما اجازه می‌دهد با کنترل از راه دور ایستگاه تلویزیون را تغییر دهیم. این انرژی در گاراژ و قفل اتومبیل را بدون کلید باز می‌کند و با امواج مایکروویو[3] غذای ما را می‌پزد. سیگنال‌های الکترومغناطیسی[4] ذاتاً امواجی هستند که از میان رسانه و بستری مانند هوا، آب، سیم‌های مسی[5]، فیبر نوری[6] و غیره انتشار می‌یابند. هر سیگنال را می‌توان با یک دامنه (باند) فرکانس‌ها

---

1. Electrical and Magnetic Energy
2. Electromagnetic Energy
3. Micro Waves
4. Electromagnetic Signals
5. Copper Wires
6. Fiber Optics

مشخص کرد که در آن، هر فرکانس مبین تعداد معینی از زمان از روی یک بستر انتقال داده‌ها است.

مؤسسات اطلاعاتی[1] از اصطلاح اطلاعات سیگنال‌ها[2] برای اشاره به دامنه وسیعی از عملیات‌ها استفاده می‌کنند که شامل رهگیری و آنالیز سیگنال‌ها در سرتاسر طیف الکترومغناطیسی[3] می‌شود. سیگنال‌ها پس از رهگیری[4] در صورت لزوم از رمز خارج شده و سپس ترجمه و تلخیص شده و آنالیز می‌شوند تا یک محصول اطلاعاتی را به‌وجود آورند که غالباً تقدیم.یکی از مقامات سطح بالا می‌شود. این روش در هنگام تحقیقات جنایی در مؤسسات مجری قانون و نیز توسط خلافکارانی که تحت تعقیب هستند، مورد استفاده قرار می‌گیرد. علاوه بر این، برخی از شرکت‌ها از این روش برای نظارت بر کارمندان خود استفاده می‌کنند.

اطلاعات سیگنال‌ها دربرگیرنده اطلاعات ارتباطات[5] و اطلاعات الکترونیکی[6] است که خود شامل استفاده از رادار[7] نیز می‌باشد. این اشکال اطلاعاتی معمولاً از نظر تکنیک‌های پردازش[8] سیگنال دیجیتالی مورد استفاده و مصرف مشترک از طیف در دامنه رادیو و رادار به هم می‌پیوندند، همچنین در حال تلفیق شدن با اطلاعات تصویری[9] هم هستند. در دسامبر سال ۱۹۹۷ مجله بین‌المللی «بررسی مسائل دفاعی جینز»[10] به تشریح راه‌اندازی مرکز ترکیبی عملیات هوایی ناتو در وینچنزای ایتالیا پرداخت، یعنی جایی‌که عملیات هوایی روزانه بر فراز بوسنی طراحی و اجرا شد. فرکانس با «هرتز» بیان می‌شود و یک هرتز عبارت است از «یک سیکل در ثانیه» و یک مگاهرتز عبارت است از یک میلیون سیکل در ثانیه. «پهنای باند» (Band Width) یعنی تفاوت میان پائین‌ترین و بالاترین فرکانس‌های موجود در یک باند.

---

1. Intelligence Agencies
2. Signals Intelligence
3. Electromagnetic Spectrum
4. Interception
5. Communication Intellignce
6. Electronic Intelligence
7. Radar
8. Orocessing Techniques
9. Imagery Intelligence
10. Jane's International Defense Review

کل دامنه فرکانس‌ها طیفی را تشکیل می‌دهند که به نام «طیف الکترومغناطیسی» معروف است. این طیف شامل (از فرکانس کم به زیاد) امواجی با فرکانس بیش از حد اندک (FLF) که برای برخی خطوط الکتریسیته و تلفن، طیف رادیویی، مادون قرمز، نور مرئی، ماورای بنفش، اشعه ایکس، اشعه گاما و اشعه‌های کیهانی به‌کار برده می‌شود. طیف‌های رادیویی، از رادیو با فرکانس پایین گرفته تا رادیو با فرکانس بیش از حد بالا و میکروویو را دربرمی‌گیرند. این طیف، شامل رادیو AM، رادیو موج کوتاه و آماتوری، رادیو دوطرفه، تلویزیون، تلفن‌های بی‌سیم، رادیو FM، رادیو سلولی (تلفن‌ها)، رادار و فرستنده‌های میکروویو می‌باشد. هر یک از دامنه‌های فرکانس، دارای مزایا و معایبی هستند. رادیو با فرکانس پایین می‌تواند از آب عبور کند، ایجاد پارازیت برای آن مشکل است و به‌شدت در برابر تداخل ایجادشده ناشی از انفجارهای هسته‌ای، مقاومت می‌کند. فرکانس‌های بالاتر معمولاً عرض باند بیشتری دارند و بنابراین، می‌توان اطلاعات بیشتری را در یک واحد به مرحله اجرا درآورد. صفحه نمایش‌های بزرگ که روی دیوارهای سفید به نمایش گذاشته می‌شد، تقریباً به‌صورت فوری تصویر عملیات هوایی تلفیقی بر فراز منطقه مورد نظر را نشان می‌داد. خصوصیات جغرافیایی منطقه با استفاده از تکنولوژی نگاشت دیجیتالی و مسیرهای پرواز هواپیماها با کمک شبکه رادار گشت هوابرد ناتو (مستقر روی زمین) اداره می‌شدند. دیگر فعالیت‌های الکترومغناطیسی در هنگام نمایش، تحت‌الشعاع قرار می‌گرفتند. این سیستم، نشان‌دهنده نوعی گرایش به سمت استفاده بیشتر از اطلاعات سیگنال‌ها به‌عنوان یکی از تجهیزات تاکتیکی بلادرنگ و صرفاً وسیله‌ای استراتژیک برای برنامه‌ریزی و خط‌مشی درازمدت است.[۱]

این موضوع دربرگیرنده کاربرد حسگرها در جمع‌آوری اطلاعات از محیط فیزیکی، سیستم‌های مخابراتی و شبکه‌های کامپیوتری است. این عملیات‌ها همگی بدون به خطر انداختن تمامیت یا در دسترس بودن بستر اطلاعاتی برای نیروهای دفاعی، دسترسی بیشتر به آن بستر را برای نیروهای تهاجمی امکان‌پذیر می‌سازد. در واقع، ممکن است نیروهای دفاعی حتی از عملیات مطلع نشوند. این بحث، همچنین به بررسی کلاهبرداری مخابراتی (که به

نیروهای تهاجمی استفاده رایگان از خدمات مخابراتی را به خرج فرد دیگری اعطا می‌کنند) و حملات فیزیکی و الکترونیکی که این خدمات را از کار می‌اندازد، می‌پردازد.

۲ـ۱ـ استراق سمع در مکالمات[1]

اکثر سیگنال‌های ارتباطی در برابر مداخله و استراق سمع آسیب‌پذیرند، به طوری‌که شنود برخی از این سیگنال‌ها نیاز به تلاش بسیاری ندارد و برخی دیگر، مستلزم ابزارهای پیشرفته و منابع قابل ملاحظه‌ای می‌باشند. از آنجایی که انجام این کار (یعنی استراق سمع) معمولاً برای افرادی که در حال برقراری ارتباط هستند، غیر قابل شناسایی است، حملاتی با چنین ماهیتی به نام حملات «انفعالی» خوانده می‌شوند، برخلاف حملات «فعالانه» که باعث جلوگیری یا اغتشاش در سیگنال‌ها می‌گردند. در بین بسیاری از ابزارهای استراق سمع می‌توان به این موارد اشاره کرد: گیرنده‌های میکروفونی[2]، دستگاه‌های ضبط صوت[3]، دستگاه‌های ضبط تلفن[4]، اسکنرهای سلولی[5]، گیرنده‌های رادیویی[6]، گیرنده‌های ماهواره‌ای[7] و میکروویو[8]، ماهواره‌های جاسوسی[9]، متجاوزان به شبکه‌های کامپیوتری[10] و فیلترهایی برای ایزوله کردن اطلاعات[11] مورد علاقه میکروفون‌های شلجمی[12] می‌توانند از یک کیلومتر دورتر مکالمات را شناسایی کنند و مدل‌های لیزری می‌توانند مکالمات را در پشت یک پنجره بسته در راستای خط دید، دریافت کنند.(۲)

تحت قانون فدرال «کنترل تلفن‌ها» در آمریکا، استراق سمع عمدی در ارتباطات الکترونیکی، سیمی یا شفاهی برای افراد، غیرقانونی است، مگر آنکه یکی از طرف‌های تحت

---

1. Eavesdropping on Conversations
2. Microphone Receivers
3. Tape Recorders
4. Telephone Tapping Devices
5. Cellular Scanners
6. Radio Receivers
7. Microwave Receivers
8. Satellite Receivers
9. Spy Satellites
10. Computer Network Sniffers
11. Filters for Isolating the Information of Intrest
12. Parabolic Microphones

نظر نسبت به این استراق سمع رضایت داشته باشد.(۳) به جز برخی از ایالت‌ها (ماننـد مریلنـد) ضبط تماس‌های خود، قرار دادن میکروفون در دفتر خود، یا حمل یک دستگاه ضبط صـوت مخفی غیرقانونی نیست و این نوع مراقبت‌ها در اغلب عملیات‌های مخفی مـورد استفاده قـرار می‌گیرند. مثلاً یک توطئه در لـس‌آنجلـس بـرای کلاهبـرداری از بانـک آمریکـا بـا استفاده از کارت‌های جعلی ATM زمانی در هم شکست که خانمی که از او دعـوت شـده بـود بـه ایـن گروه بپیوندد، طرح را به مقامات گزارش داد و قبول کرد در یکی از جلسات گروه با خود یک ضبط صوت مخفی ببرد.(۴)

همچنین این قانون فدرال تولید، فروش، نگهداری و تبلیغ تجهیزاتی که عمدتاً برای استراق سمع مخفیانه به‌کار می‌روند را ممنوع می‌داند. در هر حال، بازار بزرگی برای محصولات گشت و نظارت وجود دارد. مؤسسه Spy Factory که در یـک سـاختمان دوازده طبقـه مـستقر بـود، ظاهراً به‌عنوان بخشی از «عملیات پاکسازی»[1] FBI و به اتهام قاچـاق هـزاران دسـتگاه اسـتراق سمع به درون کشور از جمله فرستنده‌ای ریز که در خودکار، ماشین حساب، آداپتورهـای پریـز برق و جعبه‌های سیاه کوچک مخفی شده بودند و می‌شد آنها را زیر میـز، یـا در کابینـت‌هـای بایگانی، مخفی کرد، تعطیل شد. این مؤسسه، دستگاه‌های ضبط تلفنی می‌فروخت کـه مـستقیماً به خطوط تلفن متصل شده و به این طریق محتوای تماس‌هـا را بـه یـک سـایت و تجهیـزات دوردست می‌فرستادند تا در تماس‌های برقرارشده در تلفن‌های همراه، استراق سمع کننـد. ایـن دستگاه‌ها به رقبای تجاری، شرکای مظنون و همسران حسود فروخته می‌شد.(۵)

۳ـ۱ـ قانون CALEA و شنود تماس‌های تلفنی و اینترنتی

۱۲ آوریل ۲۰۰۳ کمیسیون ارتباطات فدرال به صنعت مخابراتی آمریکا دستور داد که با ارتقـای سیستم‌های خود به خصوصیات و ویژگی‌های مورد نظر FBI، دست پیـدا کنـد. پلـیس فـدرال آمریکا به کلیه شرکت‌ها تا پایان ماه برای این منظور فرصت داد. بـا اجـرای دسـتور FBI ایـن

---

1. Operation Clean Sweep

سازمان خواهد توانست کلیه مکالمات تلفنی این کشور را بدون اخذ مجوز از قاضی ضبط و استفاده کند. دستور کمیسیون ارتباطات پس از سال‌ها بحث و جدل در کمیسیون صادر شد. طی این سال‌ها، کمیسیون با FBI، گروه‌های آزادی‌های مدنی و شرکت‌های مخابراتی بر سر اجرای چنین قانونی اختلاف نظر داشتند.

سه سال پیش نیز بر سر صدور و اجرای دستوری مشابه، غوغایی عظیم برپا شد، اما از سال ۲۰۰۱ و پس از حوادث ۱۱ سپتامبر دیگر کمتر چنین واکنش‌هایی دیده شد. پس از وقایع ۱۱ سپتامبر، بسیاری از آزادی‌های مدنی آمریکا به بهانه مبارزه با تروریسم نقض شد و صدای معترضان به این امور، میان طبل جنگی که کاخ‌سفید به صدا درمی‌آورد، گم گشت.

آل گیداری[1] وکیلی که مشاور حقوقی شرکت‌های مخابراتی است، می‌گوید: «جای تأسف دارد که هیچ‌کس دستور کمیسیون فدرال را به چالش نمی‌کشد». وی گفت: «این از پیامدهای واقعه ۱۱ سپتامبر است. در زمان حاضر، دیگر کسی نمی‌خواهد برچسب ضددولت و ضدقانون را بر خود داشته باشد».

طبق قانون[2] (CALEA) که در سال ۱۹۹۴ تصویب شد، شرکت‌های مخابراتی باید با نصب دستگاه‌های خاص در دو مورد به یاری پلیس و نیروهای فدرال بشتابند، یکی در اختیار گذاشتن محتوای مکالمات و دیگری هویت مکالمه‌کنندگان. تشخیص هویت افراد در مکالمات تلفنی در آمریکا، تاکنون به دو صورت سنتی انجام گرفته است. یکی به‌صورت Penregister که با برداشتن تلفن، شماره فرد آشکار می‌شود و روش دوم Trap and Trace نام دارد که شماره فرد تماس گیرنده را آشکار می‌سازد.

مناقشه بر سر قانون CALEA و دستورالعمل پلیس فدرال آمریکا به هر حال ادامه خواهد یافت، اما مهم این است که FBI برای به‌دست آوردن هویت و شماره تلفن افراد نیازی به مجوز قاضی نخواهد داشت و تنها کسب مجوز از برخی نهادها و سازمان‌ها کفایت می‌کند.

1. Algidari
2. Communications Assistance for Law Enforcement

همچنین اگر FBI درخواست کسب اطلاعات به قاضی را بدهد و اعلام کند که به‌دلایل امنیتی نیاز به اطلاعاتی دارد، قاضی نمی‌تواند این درخواست را رد کند.

گروه‌های طرفدار آزادی‌های مدنی آمریکا از این بند قانون به‌شدت بیمناک هستند، چون اختیار عمل گسترده‌ای به FBI داده است. آنها می‌گویند، مشخص نیست که در این میان چه بر سر اطلاعات شخصی افراد می‌آید و احتمال سوءاستفاده برخی افراد و سازمان‌ها نیز وجود دارد.

این گروه همچنین معتقد است که با این روش، پلیس فدرال آمریکا به کلمات عبور، Voice Mailها و سایر اطلاعات خصوصی افراد پی خواهد برد. البته زمان طرح شکایت علیه این دستور به پایان رسیده و تنها شکایت ثبت‌شده در این مورد از طرف برخی شرکت‌های مخابراتی است که عقیده دارند، ارتقای سیستم‌ها برای رسیدن به سطحی که FBI می‌خواهد، هزینه گزافی را به آنها تحمیل می‌کند.

اما هراس بزرگی که هم‌اینک وجود دارد، اما بر زبان آورده نمی‌شود، این است که FBI از طریق کنترل تلفن‌ها به هدف بزرگ‌تری می‌اندیشد. هدف FBI، کنترل و نظارت ارتباطات اینترنتی قلمداد می‌شود.

در سال ۱۹۹۹ که کمیسیون ارتباطات فدرال به شرکت‌های مخابراتی دستور داد تا تجهیزات مورد نظر FBI را نصب کنند، اتحادیه آزادی‌های مدنی آمریکا به همراهی سه مرکز، Electronic Privacy Information Center، Electronic Frontier Foundation، Center for Democracy and Technology شکایتی را تنظیم و به دادگاه ارائه دادند. آنها از دادگاه خواستار لغو این دستور شدند و اعلام کردند که دستور کمیسیون ارتباطات فدرال، خلاف قانون مصوب کنگره بوده و هدف از این اقدامات به‌دست آوردن اطلاعات خصوصی است.

این گروه اعلام کردند که با نصب این تجهیزات، FBI توان بالای جاسوسی به‌دست می‌آورد. از طرف دیگر اتحادیه مخابراتی آمریکا نیز در همین سال به دادگاه اعلام کرد که برای رعایت استانداردهای کنگره، تجهیزات نصب‌شده، کفایت می‌کند و تغییر آنها ضرورتی ندارد.

این اتحادیه با استخدام تئودور بی‌السون[1]، مشاور کل حقوقی دولت (شخصی که نماینده دولت در دادگاه عالی است) به نبرد با این دستور رفت. نبرد اتحادیه مخابراتی در آمریکا در آگوست ۲۰۰۰ منجر به یک پیروزی بزرگ شد. دادگاه تجدیدنظر واشنگتن از ۶ مورد تقاضای FBI و FCC، ۴ مورد را رد کرد و از FCC خواست تا درباره دلایل نیاز به این تغییرات توضیح دهد. این دادگاه در حکم خود اعلام کرد: تقاضای کمیسیون ارتباطات فدرال و FBI حریم خصوصی افراد را نقض می‌کند.

با حکم دادگاه، موضوع مسکوت ماند و پلیس فدرال آمریکا برای یک سال موضوع را پیگیری نکرد. در آن زمان به‌نظر می‌رسید که موضوع از هر دو طرف پایان یافته تلقی شده، اما حملات تروریستی در آمریکا جهت‌گیری دوطرف را کاملاً تغییر داد. به‌دنبال حملات ۱۱ سپتامبر و هراس مردم از به خطر افتادن امنیت و بالا گرفتن تقاضا برای تأمین امنیت کنگره آمریکا با اکثریت آرا، قانون USA Patriot را به تصویب رساند. این قانون، اختیارات بسیاری را در دست مأموران دولتی به‌خصوص مأموران پلیس فدرال آمریکا (FBI) قرار می‌دهد. به موجب بندی از این قانون، مأموران FBI حق دارند تا از هر طریق ممکن، اطلاعات مورد نیاز خود را جمع و کلیه شرکت‌ها و سازمان‌ها وظیفه دارند، در این راه با سازمان همکاری کنند. این بند از قانون ناقض پیروزی بزرگ سال ۲۰۰۰ اتحادیه مخابراتی آمریکا بود. در سایه حملات تروریستی ۱۱ سپتامبر هیچ سازمان و گروهی در آمریکا این اختیارات را زیر سؤال نبرد و به این ترتیب دست FBI برای گسترده کردن اختیارات خود در زمینه کنترل ارتباطات بازتر شد، همچنین حملات وحشتناک تروریستی اکثریت مردم آمریکا را که همیشه به حفظ حریم شخصی خود اعتقاد داشتند، مردد گذاشت و به این ترتیب آنها بین حفظ حریم شخصی و امنیت، گزینه دوم را انتخاب کردند.

دیوید سوبل[2]، مشاور ارشد مرکز اطلاعات الکترونیکی از جمله افرادی بود که در سال ۲۰۰۰ باعث شکست FBI در دادگاه شد، می‌گوید: ما امروز هم قدرت بیش از حد FBI را زیر

---

1. Theodor B. Elson
2. David Soubel

سؤال می‌بریم. وی این ادعا را که حملات ۱۱ سپتامبر و قانون Partiot act باعث سکوت ناگهانی این مرکز و سایر مراکز مشابه در برابر این رویدادها شده، رد می‌کند و می‌گوید: سکوت و عدم فعالیت نشانه موافقت و همراهی نیست، اما ما توان به چالش کشیدن وضعیت فعلی را نداریم.

او از رأی دادگاه تجدید نظر در سال ۲۰۰۰ تمجید می‌کند و می‌گوید: تصور می‌کردیم با آن رأی موضوع خاتمه یافته است. جری برمن[1]، مدیر مرکز دموکراسی و تکنولوژی نیز می‌گوید: موضوع حفظ حریم شخصی هنوز برای ما و اکثر مردم مهم است، اما تغییرات به‌وجود آمده پس از حوادث ۱۱ سپتامبر پیگیری این موضوعات را سخت کرده است.

وی مراجعه مجدد به دادگاه در مقطع فعلی را رد می‌کند و می‌گوید: قضات با استناد به قوانین جدید می‌توانند ورق را کاملاً به نفع FBI برگردانند. وی بر این باور است که در مقطع زمانی حاضر، گروه‌های طرفدار آزادی‌های مدنی شانس بسیار کمی دارند.

برمن می‌گوید: به‌دنبال این رویدادها ما کاملاً محاصره شده‌ایم. وزارت جدید امنیت کشور، قوانین جدید وضع‌شده از سوی مجلسین آمریکا و ساختار جدید FBI، همه باعث گشته تا وضعیت ما دشوارتر شود.

به گفته وی، اگر زمان مانند قبل از ۱۱ سپتامبر بود، مطمئناً همه را رد می‌کردیم و با آنها مبارزه می‌نمودیم. اما امروزه اولویت‌ها تفاوت نموده و ما نمی‌توانیم مانند قبل عمل کنیم. جیمز دمپسی نیز از مرکز CDT می‌گوید: ما مخالف عملکرد FBI بوده و هستیم. وی از اینکه کمیسیون ارتباطات فدرال با وضع قوانین جدید از حدود خود تجاوز کرده، اظهار تأسف می‌کند و می‌گوید: قوانین جدید فراتر از چیزی است که کنگره وضع کرده بود. پلیس فدرال آمریکا هم‌اکنون اختیارات گسترده‌ای دارد. به‌عنوان مثال، کلیه خطوط تلفن همراه ردیابی می‌شود و شرکت‌ها موظف هستند کلیه آمار و اطلاعات درخواستی سازمان‌های دولتی را در اختیار آنها بگذارند. همچنین با نصب تجهیزات جدید FBI، این امکان وجود دارد تا به محض

1. Jerri Berman

اینکه فردی شماره‌گیری می‌کند، شماره و ریز مکالمات او را دریافت کنند. حتی این سازمان می‌تواند مکان کلیه افرادی را که از تلفن‌های عمومی زنگ می‌زنند، ردیابی نماید.

اما سؤالی که این‌بار برای بسیاری مطرح می‌شود، این است که چرا شرکت‌های مخابراتی، تسلیم شده‌اند. مایک آلتشول[1]، مشاور ارشد شرکت Cellular Telecommunication and Internet می‌گوید: FBI این‌بار از طریق قانون وارد شده و کنگره و کمیسیون ارتباطات فدرال و قانون از خواسته‌های آنها حمایت می‌کنند. هم‌اکنون کلیه شرکت‌های مخابراتی آمریکا موظفند تا در تجهیزات فنی خود تغییرات درخواستی FBI را ایجاد کنند و FBI هم هزینه این تعمیرات را می‌پردازد. به گمان بسیاری از گروه‌های مدنی در آمریکا، FBI از شرایط پس از حوادث ۱۱ سپتامبر به خوبی استفاده کرد و توانست با استناد به قانون، آزادی‌های مدنی را محدود کند. این گروه‌ها اذعان دارند که پس از این حملات، غافلگیر شدند و نتوانستند واکنش مناسبی نشان دهند.

FBI هم‌اکنون این قدرت را دارد تا بر کلیه وسایل ارتباطی نظارت کامل اعمال کند، اگرچه قانون CALEA تنها به‌منظور کنترل تلفن‌های همراه بود، اما این سازمان، کنترل را به اینترنت نیز تعمیم داده و قوانین جاسوسی تلفن به اینترنت نیز تسری یافته است. FBI خود معتقد است که طبق قوانین مصوب کنگره، کنترل و نظارت بر کلیه راه‌های ارتباطی را دارد و این شامل تلفن، اینترنت و هرّ وسیله دیگری است. به گفته آل گیداری[2] از دید FBI، قوانین به معنای آن است که تماس تلفنی شما شنیده می‌شود، شماره تلفن شما ضبط می‌گردد، اینترنت شما زیر نظر است و نامه‌های شما خوانده می‌شود. به‌نظر شما دنیای آزاد کجا است؟(۶)

۴ـ۱ـ شنود ارتباطات[3] در اتحادیه اروپا

در اتحادیه اروپا یک اصل کلی مبنی بر محرمانه بودن ارتباطات (و جریان‌های اطلاعاتی مربوط

---

1. Mike Altcshoul
2. Algidari
3. Eavesdropping of Communication

به آن) وجود دارد . استراق سمع ارتباطات ممنوع است، مگر در شرایطی خاص با اهدافی مشخص و مجوز قانونی. این اصل از بند ۸ کنوانسیون اروپایی در مورد حقوق‌بشر که در بند ۶ معاهده اتحادیه اروپا و به‌طور اخص در دستورالعمل‌های ۹۵/۴۶ و ۹۷/۶۶ کمیسیون اروپا به آن اشاره شده، پیروی می‌کند.

تمام کشورهای عضو اتحادیه دارای چارچوبی حقوقی هستند که بر آن اساس می‌توانند مجوز قضایی (یا در دو کشور عضو، مجوزی که به‌طور شخصی از سوی یک کاردار ارشد صادر شده بود) برای شنود مطالب موجود بر روی شبکه‌های عمومی ارتباطات راه دور را به مراجع انتظامی خود بدهند. این چارچوب قانونی باید همسو با حقوق جامعه اروپایی باشد تا بتواند به اندازه‌ای کاربردی گردد که شامل مواردی برای حفاظت از حقوق زیربنایی اشخاص بر حریم خصوصی خود می‌باشد که عبارتند از: محدود کردن استراق سمع به موارد پی‌جویی جرائم خطرناک، الزام به حفظ ضرورت و تناسب شنود در پی‌جویی‌های فردی، یا اطمینان از حصول اطلاع شخص مورد نظر از روند شنود به محض دفع احتمال اختلاف در بازجویی. در بسیاری از کشورهای عضو اتحادیه، قانونگذاری مربوط به شنود، الزاماتی را برای عاملان ارتباطات راه دور (خدمات عمومی) مبنی بر ایجاد قابلیت‌های استراق سمع به‌وجود می‌آورند. هدف یکی از قطعنامه‌های ۱۹۹۵ شورا هماهنگ کردن شروط شنود بود.

در گذشته، کارکنان شبکه‌های ارتباطی سنتی، به‌ویژه مسئولان خدمات صوتی، با مراجع انتظامی دارای روابط کاری بودند تا از آن طریق، شنود مشروع ارتباطات را میسر سازند. شکست انحصار ارتباطات راه دور و انفجار استفاده از اینترنت، افراد بسیاری را به بازار جلب کرده است، اما باز هم با شروط و الزامات شنود روبرو شده‌اند. مسائل مربوط به مقررات، امکانات فنی، تخصیص هزینه‌ها و اثرات تجاری باید در گفت‌وگوهای دولت و بخش صنعت با تمام گروه‌ها و احزاب دخیل، شامل مراجع ناظر بر حفاظت از اطلاعات مطرح و مورد بحث قرار گیرند.

فناوری‌های جدید، کشورهای عضو اتحادیه را ملزم می‌سازد تا در صورت تمایل

توانایی‌های خود در انجام شنود قانونی ارتباطات را حفظ کنند و با یکدیگر همکاری نمایند. در حالی‌که اعضای اتحادیه، شروط فنی جدیدی برای عوامل ارتباطات راه دور و تأمین‌کنندگان خدمات اینترنتی در مورد شنود ارائه می‌دهند، اما کمیسیون بر این باور است که این اصول برای جلوگیری از ایجاد اخلال در بازار واحد، به حداقل رساندن هزینه‌های بخش صنعت و رعایت حریم خصوصی و شروط حفاظت از اطلاعات، باید در سطح بین‌المللی و به‌صورت هماهنگ انجام شوند. این استانداردها باید در صورت امکان، عمومی و باز بوده و نباید باعث بروز ضعف در زیرساخت‌های ارتباطاتی شوند. در چارچوب کنوانسیون اتحادیه اروپا درمورد همیاری مشترک در مسائل کیفری، اعضای اتحادیه در خصوص اتخاذ رویکردی واحد در همکاری برای شنود قانونی، توافق کرده‌اند. این کنوانسیون، حاوی قواعد پیش‌بینی‌شده‌ای برای شنود ارتباط تلفنی ماهواره‌ای و استراق سمع ارتباطات یک فرد در درون حوزه استحفاظی کشوری دیگر از اعضای اتحادیه می‌باشد. کمیسیون اروپا معتقد است که قواعد مربوط به شنود که در کنوانسیون همکاری قانونی دوجانبه پیش‌بینی شده است، در وضعیت جاری بیشترین میزان استراق سمع را مجاز می‌داند. متن مکتوب این کنوانسیون در حال حاضر یک فناوری بی‌اثر است (تنها جملاتی بر روی کاغذ است)، قبل از در نظر گرفتن هرگونه تغییر در این متن، ابتدا باید در عمل سنجیده شود. کمیسیون اجرایی، این کنوانسیون را با اعضای اتحادیه اروپا، کاربران و مراجع ناظر بر حفاظت از اطلاعات شخصی بررسی خواهد کرد تا اطمینان حاصل شود که اقدامات اولیه مؤثر، شفاف و متوازن بوده‌اند.

استفاده مغرضانه و نابجا از قابلیت‌های شنود، به‌ویژه در سطح بین‌المللی، مسائل مربوط به حقوق‌بشر را پیش خواهد آورد و اعتماد شهروندان به جامعه اطلاعاتی را کمرنگ خواهد نمود. کمیسیون با پیگیری مداوم شاهد گزارشاتی در خصوص استفاده نادرست از قابلیت‌های شنود بوده است.

به‌منظور استراق سمع در یک خط تلفن استاندارد، فرد اقدام‌کننده باید یک نقطه اتصال فیزیکی مانند یک اتاقک تلفن و یا به یک سوئیچ کامپیوتری دسترسی پیدا کند تا تماس‌ها از طریق آن،

مسیریابی شوند. با افزایش استفاده از فیبرهای نوری[1] (رشته‌های میکروسکوپی که به‌صورت هزارتایی کنار هم قرار گرفته‌اند تا ترافیک محلی و نیز راه دور را انتقال دهند). دسترسی فیزیکی به خود «سیم‌ها» عملاً غیرممکن می‌شود. رسانه‌های بریتانیا گزارشی را در مورد توطئه‌ای برای سرقت شماره حساب ATM و شماره شناسنامه شخصی از طریق دستگاه‌های ضبط مکالمات تلفنی منتشر کردند. این توطئه در زندان و در نزد گروهی از گانگسترهای باتجربه و دلالان موادمخدر و یک کارشناس نرم‌افزار (که مدتی را به‌علت حمله به همسر و فرزندش زندانی شده و مجبور به همکاری در این نقشه گشته بود)، ریشه گرفت. آن مرد نقش خود را به رئیس زندان لو داد و بعدها به‌صورت یک خبرچین مخفی به فعالیت خود ادامه داد. در مورد دیگری که در انگلستان به وقوع پیوست، فردی حق‌السکوت بگیر در معاملات رمزگذاری شده بانک، استراق سمع می‌کرد. گفته می‌شود وی بعد از شکستن کد مورد نظر با موفقیت، ۳۵۰ هزار پوند را از بانک به چنگ آورده است.(۷) در ایران نیز اگرچه هنوز بانکداری الکترونیکی E-Banking به مرحله اجرا درنیامده، اما بخش‌هایی از آن مانند استفاده از دستگاه‌های ATM به‌صورت محدود در ایران پیاده‌سازی شده است. با وجودی‌که این دستگاه‌ها به اینترنت متصل نیستند و خود دارای یک شبکه رایانه‌ای مستقل هستند، اما یک نفوذگر رایانه‌ای توانست در تابستان ۱۳۸۲ به شبکه مذکور نفوذ کرده و ده‌ها میلیون تومان پول از صاحبان حساب‌ها به سرقت ببرد. گزارش کاملی از این رویداد در فصل سوم همین مجلد ارائه شده است.

یکی دیگر از شگردهای هکرهای کامپیوتری، نفوذ به کامپیوترهای شرکت‌های تلفن است تا از این طریق بر خطوط تلفنی نظارت غیرمجاز داشته باشند.

گروه‌های جنایی سازمان‌یافته به کرات در ارتباط‌های نیروی پلیس استراق سمع می‌کنند تا نسبت به هوشیاری پلیس در برابر فعالیت‌های خود آگاهی داشته باشند. مثلاً یکی از سازمان‌های جنایی هلند بر شبکه‌های پیجر پلیس نظارت داشته و خطوط تلفن خانه‌های امن و منازل مقامات عالی پلیس را ضبط می‌کرد.(۸)

---

1. Fibre Optical

در میانه دهه ۸۰ میلادی مقامات ایالت‌های تگزاس و فلوریدا تأسیساتی که مجهز به وسایل نظارت بر سیگنال‌ها بود، یافتند از جمله اسکنرها و انواع گیرنده‌ها. فرکانس‌های مورد هدف، شامل فرکانس‌های متعلق به سیستم مجری قانونی محلی و فدرال بودند؛ رادیو تک کانالی VHF (فرکانس بسیار بالا) و UHF (فرکانس بیش از حد بالا) هدف ظاهری این بوده که نسبت به فعالیت‌های مبارزه با موادمخدر از جمله شناسایی معاملات مواد و حملات قریب‌الوقوع هشدارهایی به‌دست آورند. لاگ‌های[1] استراق سمع و دیگر رکوردهای مکتوب نشان می‌دادند که این تأسیسات به‌دست پرسنل سابق نیروی دریایی و ارتش اداره شده است.(۹) پلیس کلمبیا و مأموران اداره مبارزه با موادمخدر در زمان حمله به دفاتر مرکزی Cali طی یکی از عملیات‌های قاچاق مواد، مواردی مانند تجهیزات اسکن سیگنال برای استراق سمع مکالمات تلفنی، پیام‌های فاکس و عملیات کنترل ترافیک هوایی را پیدا کردند. همچنین نیروهای این اداره جت‌های کلمبیایی بارگیری شده با موادمخدر را کشف نمودند که مجهز به وسایل استراق سمع هوا به هوا بودند تا بر مسیرهای مربوط به جت‌های نظامی آمریکا که بر فراز خلیج مکزیک و دریای کارائیب پرواز می‌کنند، نظارت داشته باشند.(۱۰)

حدود ۹٪ پاسخ‌دهندگان به نظرسنجی FBI در سال ۱۹۹۸ موسوم به «امنیت و جرائم کامپیوتری»[2] گزارش کردند که در طول سال گذشته متوجه استراق سمع مخابراتی شده‌اند. در بین آنها ۱۰ نفر خسارت‌های قابل ملاحظه‌ای را از هزار تا دویست هزار دلار گزارش دادند که متوسط رقم آن به ۵۶ هزار دلار می‌رسد.(۱۱)

۵ـ۱ـ استراق سمع سلولی[3]

تماس‌های مربوط به تلفن‌های سلولی (همراه) به شدت در برابر استراق سمع آسیب‌پذیرند، زیرا سیگنال‌های آنها در هوا و در بین تلفن کاربر و یک برج فرستنده ـ گیرنده میکروویو در

1. Logs
2. Computer Security and Crimes
3. Cellular Intercepts

همان نزدیکی در رفت و آمد هستند. (از آنجا این تماس‌ها از روی سیم‌هایی که وارد شبکه تلفن سوئیچی عمومی می‌شوند مسیریابی می‌شوند). یک اسکنر نسبتاً ارزان قیمت، اقدام به بررسی امواج هوایی می‌کند تا تماس‌ها را جست‌وجو کرده و روی یکی از آنها قفل کند. با دستگاهی به نام «ردیاب تماس‌ها» فرد شنود کننده می‌تواند در مکالماتی که در هر تلفن سلولی به‌خصوص در محدوده یک سایت سلولی مجاور به وقوع می‌پیوندد Zero in کند. شماره تلفن هدف از طریق صفحه کلید وارد دستگاه می‌شود. مؤسسات اطلاعاتی و مجریان قانون می‌توانند دستگاه‌های پیشرفته‌تری داشته باشند. مثلاً شرکت Law Enforcement در نیویورک سیستمی را تبلیغ می‌کند که بر ۱۹ کانال نظارت دارد و به‌طور همزمان رد سه مکالمه را می‌گیرد.(۱۲)

چندین مورد رویدادهای تصادفی هم گزارش شده که این نوع اسکنرها در آن دخیل بوده‌اند، از جمله مواردی که مکالمات خصوصی اشخاص برجسته دولتی را افشا کرده‌اند. در سال ۱۹۹۵ مکالمه تلفنی یکی از مدیران بازنشسته بانک در آکسفورد شنود شد و یک تماس تلفن سلولی بین شاهزاده دیانا و دوست نزدیکش، جیمز گیلبی که وی را نوگل عزیزم خطاب می‌کرد، ضبط شد. این مکالمه ۲۳ دقیقه‌ای از روی نوار پیاده شده و در مجله Sun منتشر گشت. شاهزاده چارلز نیز با افشای مکالمات تلفنی ضبط شده دچار دردسر شد. در یک مورد وی زندگی سکسی را با کاملیا مورد بحث و بررسی قرار داده بود. در سال ۹۶ مکالمه‌ای تلفنی بین رئیس مجلس نمایندگان آمریکا، نیوت گینگریچ و دیگر اعضای کادر رهبری جمهوری‌خواهان در کنگره، ضبط شده و در رسانه‌های خبری انتشار یافت. در نیوهمپاشایر، یکی از فعالان ضدهسته‌ای تماس‌هایی را که از اتاق کنترل[1] در تأسیسات هسته‌ای[2] Seabrook گرفته می‌شود (از جمله یکی از افرادی که می‌گفت «من نسبت به این سوپاپ‌ها احساس بدی دارم») ضبط کرد.(۱۳)

با وجودی‌که قانون سال ۱۹۹۴ کار واردات، تولید و فروش اسکنرهای سلولی را در آمریکا ممنوع اعلام کرد اما یک اسکنر رادیویی قانونی را در عرض یک دقیقه و با کمک یک تکه

---

1. Control Room
2. Nuclear Plant

سیم دو اینچی و هوویه لحیم کاری می‌توان تبدیل به وسیله‌ای کرد که تماس‌های سلولی را دریافت می‌کند. در جلسات کمیته فرعی مخابرات در کمیته تجارت مجلس نمایندگان آمریکا، رئیس این کمیته به نام بیلی تاوزین، نشان داد که ساخت اسکنر و دریافت یک تماس تلفنی تا چه اندازه آسان است.(۱۴) باب گراو که شرکتش این‌گونه خدمات دستکاری را ارائه می‌دهد، شهادت داد که از ۱۰ میلیون اسکنر قانونی فروخته‌شده در آمریکا تخمین زده می‌شود که دویست ـ سیصد هزار عدد از آنها دستکاری شده‌اند تا فرکانس‌های سلولی را رهگیری کنند. دستورالعمل انجام این‌گونه دستکاری‌ها در اینترنت و برخی از مجلات در دسترس هستند. قانون سال ۱۹۹۴ می‌خواهد که اسکنرهای رادیویی جدید طوری طراحی شوند که نتوان آنها را به آسانی دستکاری کرد تا تماس‌های سلولی را رهگیری کنند، اما «سازمان صنایع مخابرات سلولی»[1] خواهان قوانین سخت‌تر برای پوشش تکنولوژی‌های جدید است. تلفن‌های همراه دیجیتالی جدید از تکنولوژی‌هایی بهره می‌گیرند که کار اسکن کردن را بسیار دشوار می‌کنند. سیگنال‌ها به مراتب پیچیده‌تر هستند و ممکن است برای جلوگیری از سوءاستفاده از مکالمات بدون دانستن کلید مخفی[2]، از رمزنگاری[3] استفاده شود.(۱۵)

۶ـ۱ـ شنود در پیجر[4]

می‌توان با یک پیجر مشابه‌سازی شده (پیام‌هایی را که برای یک پیجر به‌خصوص هدایت می‌شوند را گرفت) پیام پیجرها را از روی هوا دریافت کرد. بنا به گفته یکی از مقامات سرویس مخفی آمریکا، مجموعه کاملی از تجهیزات که شامل دستگاه استراق سمع پیجر، یک کامپیوتر با نرم‌افزار مخصوص و اسکنر می‌باشد به قیمت ۳۰۰ تا ۱۰۰۰ دلار قابل خریدن است.(۱۶)

در ماه اوت سال ۱۹۹۷، سه مرد متهم به استراق سمع غیرقانونی در پیام‌های محرمانه

---

1. The Cellular Telecommunications Industry Association
2. Sectet Key
3. Encryption
4. Pager Intercepts

مقامات ارشد در دفتر شهردار، اداره پلیس، آتش‌نشانی، گروه خنثی‌کننده بمب و دفتر یکی از دادستان‌های منطقه در شهر نیویورک شدند. پیام‌ها (که بیش از آن حساس بودند که با رادیوی پلیس ارسال می‌شوند) شامل محل‌های زندگی مقامات سطح بالای دولتی و فدرال، مخفیگاه‌های شاهدان جنایت و تحقیقات و تعلیقات افسران پلیس بود.(۱۷) این افراد برای شبکه Breaking News (یکی از سرویس‌های محلی که روزنامه، ایستگاه تلویزیونی و سرویس‌های سیمی همراه با اطلاعاتی که معمولاً از رادیوی پلیس مانند تماس‌های پلیس و آتش‌نشانی به‌دست می‌آیند، ارائه می‌کنند) کار می‌کردند، یا صاحب آن بودند. مقامات BNN اعلامیه‌ای منتشر ساختند و ضمن انتقاد از این دستگیری‌ها اعلام کردند که پرونده دولت براساس «اطلاعاتی بوده که ممکن است به‌دست دو نفر از داوطلبان ناراضی و سابق جعل شده باشد که شش ماه قبل از شرکت جدا شده و یکی از آنها در ملأ عام سوگند خورد که شرکت را نابود خواهد کرد». دفتر دادستان آمریکا که این کار تحقیقاتی را با نام رمز «عملیات پیجر گیت» نامگذاری کرده بود، اعلام نمود از یک «خبرچین معتمد» یک پیجر شبیه‌سازی شده به‌دست آورده است.(۱۸)

۷ــ۱ــ ضبط مکالمات تلفنی برای اجرای قانون[1]

با وجودی‌که در آمریکا، استراق سمع مکالمات خصوصی غیرقانونی است، اما دولت فدرال و دولت‌های ۳۷ ایالت این کشور از طریق قوانین فدرالی و ایالتی اجازه یافته‌اند تا تحت شرایط خاصی (که شامل کسب حکم دادگاه براساس علت احتمالی یک فعالیت جنایی و فقط گوش دادن به مکالمات مربوط می‌باشد)، اقدام به استراق سمع در مکالمات سیمی و الکترونیکی نمایند.(۱۹) این قوانین طوری طراحی شده‌اند که حفاظت از حریم خصوصی و حقوق مندرج در متمم اول قانون اساسی تضمین شده و در عین حال استفاده از دستگاه‌های ضبط مکالمه تلفنی و میکروفون‌های استراق سمع برای تحقیق در فعالیت‌های جنایی و اطلاعات خارجی

---

1. Law Enforcement Wire Taps

امکان‌پذیر شود. ملزومات حقوقی، ریشه در دو مورد از قوانین موضوعه فدرال دارند: قانون «کنترل فراگیر جرائم و خیابان‌های امن» که در سال ۱۹۶۸ به تصویب رسید و با قانون «حریم خصوصی ارتباطات الکترونیکی» در سال ۱۹۸۶ اصلاح شد تا دربرگیرنده ارتباطات الکترونیکی نیز باشد و قانون «نظارت بر اطلاعات خارجی» که در سال ۱۹۷۸ به تصویب رسید. قانون اول دربرگیرنده تحقیقات جزایی بوده و قانون دوم به امور اطلاعاتی و عملیات‌های ضداطلاعاتی می‌پردازد.[۲۰] قانون اخیر، متعاقب گزارش کمیته Church به سال ۱۹۷۴ (کمیته منتخب سنا برای مطالعه عملیات‌های دولتی با توجه به فعالیت‌های اطلاعاتی) که نشان می‌داد محافل اطلاعاتی در نظارت گسترده بر آمریکایی‌ها از جمله پدر روحانی، مارتین لوتر کینگ پسر، درگیر شده‌اند به تصویب رسید.[۲۱]

مراقبت الکترونیکی و به‌خصوص استراق سمع تلفنی در تحقیقات جنایی متعددی مورد استفاده قرار گرفته است، از جمله مواردی که شامل جرائم سازمان‌یافته، قاچاق موادمخدر و فساد دولتی می‌باشند. این نوع ضبط مکالمات تلفنی می‌تواند به‌شدت ارزشمند باشد، زیرا سخنان خود سوژه را ضبط می‌کنند ونقشه‌ها و نیات او را برملا می‌سازند. مدارک به‌دست آمده از طریق نظارت و مراقبت الکترونیکی معمولاً بهتر از اطلاعات به‌دست آمده از طریق مثلاً خبرچین‌ها (که عمدتاً خودشان خلافکار بوده و به‌شدت غیرقابل اتکا هستند) در دادگاه تأثیرگذار واقع می‌شوند.[۲۲]

بعضی تبهکاران تلاش کرده‌اند تا با عدم استفاده از تلفن از دست مجریان قانون بگریزند. وقتی این کار را می‌کنند نیروهای پلیس باید به سراغ ابزارهای پرنفوذتری بروند.[۲۳]

نظارت الکترونیکی در پرونده‌های تروریستی نیز مفید واقع شده و در مواردی هم به جلوگیری از حملات مرگبار کمک کرده است.[۲۴]

در سال ۱۹۹۷ دادگاه‌های آمریکا تعداد ۱۱۸۶ مورد تقاضانامه برای ضبط مکالمات جنایی را تأیید کردند که ۷۳٪ آنها برای توجیه درخواست حکم، موادمخدر را به‌عنوان جدی‌ترین جرم ذکر کرده‌اند.[۲۵]

در اکتبر سال ۱۹۹۴ کنگره آمریکا قانون «همکاری مخابراتی برای اجرای قانون» را به تصویب رساند که در ابتدای امر به نام «لایحه ارتباط تلفنی دیجیتال» معروف بود. هدف اصلی لایحه، تضمین این نکته بود که مؤسسات مجری قانون در زمانی که تکنولوژی‌ها و سرویس‌های جدید (مانند سرویس‌های ارتباطی شخصی و بی‌سیم) مستقر می‌شوند، همچنان به ارتباط تلفنی دسترسی خواهند داشت.(۲۶)

۸ـ۱ـ رهگیری اطلاعات خارجی[1]

مؤسسات اطلاعاتی ملی[2] از اطلاعات سیگنال برای جمع‌آوری اطلاعات خارجی درباره متحدان و دشمنان خود استفاده می‌کنند. در آمریکا این مؤسسات مجاز نیستند تا در مورد شهروندان آمریکایی به جمع‌آوری اطلاعات بپردازند (به جز تحت قانون نظارت بر اطلاعات خارجی و با حکم دادگاه) اما اجازه دارند مکالمات افراد خارجی در آن سوی آب‌ها را کنترل نمایند. وظیفه انجام این کار، عمدتاً بر عهده «آژانس امنیت ملی» (NSA) است که ستاد مرکزی آن در فورت میده مریلند است. دستگاه‌های این آژانس، دنیا را تحت پوشش دارند و مکالماتی را که برای منافع ملی مهم به‌نظر می‌رسند از فعالیت‌های تروریستی[3] و تکثیر تسلیحات[4] گرفته تا مذاکرات تجاری[5] ضبط می‌کنند. شنودهای این آژانس، به تحقیقات مربوط به جرائم سازمان‌یافته جهانی[6] کرده است.(۲۷)

آژانس امنیت ملی طوری مجهز شده تا بر هر چیز از ارتباطات ماهواره‌ای و میکروویو[7] گرفته تا خطوط زمینی و ارتباطات رادیویی[8] نظارت داشته باشد. پروژه موسوم به Yogurt که این آژانس راه‌اندازی کرده بود تا در سیستم‌های واکی تاکی[9] که مورد استفاده تروریست‌ها،

---

1. Foreign Intelligence Intercepts
2. National Intelligence Agencies
3. Terrorist Activity
4. Weapons Proliferation
5. Trade Negotiations
6. Microwave and Satellite Communications
7. Radio Communications
8. Walkie - Talkies
9. Donken Campbell

سربازان خارجی و افسران پلیس بوده و در یک قاب قابل حمل، دارای گیرنده رادیویی، جهت یاب، کامپیوتر و دستگاه ضبط هستند، نفوذ کنند. گستره جهانی این آژانس تا حدودی ناشی از مشارکت آن در طرح Echelon (اشلون) است. این طرح یک سیستم نظارت جهانی، تحت اداره ۵ کشور متشکل از آمریکا، انگلستان، کانادا، استرالیا و نیوزیلند است.(۲۸) این شبکه تأسیسات شنیداری که در سال ۱۹۸۸ به‌دست دانکن کمپبل[1] در مجله News Stateman افشا گشت و در سال ۱۹۹۶ به دست نیکی هاگر[2] در مجله Secret Power به‌طور کامل و مستند تشریح شد، شامل ایستگاه‌های استراق سمع ماهواره‌ای، ایستگاه‌های زمینی میکروویو، ماهواره‌های جاسوسی، پست‌های گوش دادن به رادیو و تأسیسات مخفی است که مستقیماً به شبکه‌های مخابراتی زمینی متصل می‌گردند.(۲۹) این آرایش عظیم آنتن‌ها و دستگاه‌های رهگیری اقدام به دریافت ارتباطات صوتی، فاکسی و داده‌هایی می‌کنند که در سیستم‌های مخابراتی جهانی در تردد هستند. بزرگ‌ترین ایستگاه به نام منویت هیل، تحت اداره آژانس امنیت ملی است و در منطقه نورث یورک مورز[3] در شمال انگلستان قرار دارد. این تأسیسات با ۲۲ ترمینال ماهواره‌ای و تقریباً ۵ جریب ساختمان، در حکم یک ایستگاه زمینی برای ماهواره‌های جاسوسی آمریکا است که اقدام به رهگیری خطوط میکروویو و دیگر ارتباطات کوتاه‌برد مانند رادیوهای نظامی[4] و دستگاه‌های واکی تاکی می‌کنند. سایر ایستگاه‌های شنود ماهواره‌ای در شوگر گراو[5] در ویرجینایّ غربی، یاکیما[6] در ایالت واشنگتن، مورونستاو[7] در انگلستان، ژرالد تون[8] در استرالیای غربی و وایهوپی[9] در نیوزیلند قرار دارند.(۳۰)

سیستمی با ساختار پیشرفته به دقت کنترل می‌کند که کدام پیام‌ها نگهداری شوند و چه افرادی به آنها دسترسی دارند. اکثر پیام‌ها به‌وسیله یک فرآیند تصفیه کامپیوتری[10] به سرعت

1. Nikky Hagger
2. North York Morez
3. Military Rodios
4. Shoger Grow
5. Yakima
6. Moronstow
7. Geraldton
8. Waihoppy
9. Computerized Filtering Process
10. Potential Terrorists

دور ریخته می‌شوند. وقتی پیام‌ها دریافت می‌گردند، از یک کامپیوتر فرهنگ لغت که برای بررسی کلمات کلیدی خاص برنامه‌ریزی شده‌است، عبور داده می‌شوند.(۳۱) این لغت‌نامه از روی مقولات شنیداری که مؤسسات اطلاعاتی این ۵ کشور تهیه کرده‌اند، استنباط شده است. هر مقوله دارای فهرستی از ۱۰ تا ۵۰ کلیدواژه است که برای انتخاب پیام‌هایی برای همان مقوله مورد استفاده قرار می‌گیرند. کلیدواژه‌ها شامل مواردی، مانند اسامی مردم، کشتی‌ها، سازمان‌ها، کشورها، شماره‌های تلفن، آدرس‌های اینترنتی و کلمات موضوعی هستند. این مؤسسات ترکیبات خاصی از کلیدواژه‌ها را نیز تعیین می‌کنند مثلاً «سووا» و «کمک» یا «سووا» و نه «مشورت» (سووا پایتخت فیجی است). وقتی پیامی با معیارهای خاص یکی از مقولات تطبیق داده شد، مهر کد چهار رقمی دیجیتالی این مقوله و کد کامپیوتر لغت‌نامه‌ای که آنرا پردازش کرده به آن می‌خورد، سپس به طرف آژانسی هدایت می‌شود که آن کد را عرضه کرده است و در غیر این صورت آنرا کنار می‌گذارند. مسائل اطلاعات نظامی و سیاسی جزو اولویت‌های اصلی هستند، اما پیام‌هایی که مربوط به تروریست‌های بالقوه[1] و اطلاعات اقتصادی[2] می‌شوند نیز از قلم نمی‌افتند.(۳۲)

این اتحاد ۵ کشوری از روز تلاش‌های همکارانه در زمان جنگ جهانی دوم رشد کرده و به مرحله شنود ارتباطات رادیویی رسیده است. این سیستم به‌عنوان موافقت‌نامه UKUSA در سال ۱۹۴۸ به‌صورت رسمی مطرح شد و انگلستان وآمریکا جزو امضا کنندگان و شرکای اصلی و کشورهای استرالیا، کانادا و نیوزیلند شرکای درجه دوم محسوب شدند. این توافق‌نامه، کره زمین را به ۵ سپر تقسیم کرد و هرکس موظف به نظارت بر اهداف خاصی شد. مثلاً بریتانیا، مسئول شنود پیام‌های چین شد.(۳۳)

وجود سیستم Echelon باعث ناراحتی قابل ملاحظه‌ای در بین اروپائیان شده است چرا که می‌ترسند آژانس امنیت ملی آمریکا از آن برای جاسوسی تجاری و نظامی استفاده کند. آلمان

1. Potential Terrorists
2. Economic Intelligence

به‌طرز خاصی نسبت به ایستگاه مجاور منویت هیل[1] که در منطقه بادآیبلینگ[2] آلمان مستقر شده نگران است. آژانس امنیت ملی، منکر جاسوسی در کشورهای اروپایی به نفع شرکت‌های آمریکایی شده است.[۳۴]

روسیه یکی از بزرگ‌ترین تأسیسات اطلاعات در ارتباطات دنیا را در نزدیکی هاوانا (کوبا) یعنی حومه لوردز اداره می‌کند. این تأسیسات که در دهه ۷۰ میلادی ساخته شدند برای شنود ارتباطات نظامی، دیپلماتیک و تجاری در شرق ایالات‌متحده و در بخشی از میدوست[3] و نیز ترافیک بین آمریکا و اروپا مورد استفاده قرار می‌گیرد. این سیستم می‌تواند امواج سلولی، میکروویو و رادیویی را تا حداکثر هزار مایل دورتر دریافت کند. فرماندهی مرکزی آمریکا در تامپا فلوریدا که بر نیروهای آمریکایی در خاورمیانه نظارت دارد در محدوده برد این سیستم قرار دارد. ارتباطات انجام‌شده در غرب آمریکا و Pacific Basin از تأسیسات مشابهی در ویتنام کمونیست، شنود می‌شوند. تأسیسات لوردز، تحت اداره مدیریت اصلی اطلاعاتی متعلق به ستاد فرماندهی نیروهای نظامی روسیه می‌باشد که حدود ۲۰۰۰ نفر از متخصصان اطلاعاتی در این تأسیسات مشغول خدمت هستند. بنا به گفته یکی از مقامات نظامی شوروی سابق به نام استا نیسلاو و لونف[4]، مقامات کرملین از طریق دستگاه‌های شنود شوروی در لوردز از نقشه‌های جنگی آمریکا برای جنگ خلیج‌فارس مطلع شدند.[۳۵] لونف می‌گوید، آنها گفت‌وگوهای خلبانان هوآپیماهای جنگی آمریکا در هنگام پرواز و مکالمات شخصی بین سربازان و خانواده‌هایشان را دریافت می‌کردند.[۳۶]

ژاپن در سیراهو[5] در جزیرهٔ وایشیگاگی[6] در شمال شرق تایوان، تأسیسات استراق سمع بزرگی را اداره می‌کند. این تأسیسات که به‌طرز مطلوبی برای شنود ترافیکی[7] در کره جنوبی و تایوان برقرار شده، مستقر گشته است. ژاپنی‌ها همچنین ایستگاه‌های شنود در جزیره ریبان و

1. Menwite Hill
2. Bad Aiblinge
3. Midwest
4. Stanislav Lunev
5. Sirahoo
6. Vishigagi
7. Inter Cepting Traffic

لیگایگاشیما را اداره می‌کنند که برای شنود پیام‌های آمریکایی که به ژاپن وارد یا خارج می‌شوند، مورد استفاده قرار می‌گیرد. گفته می‌شود شرکت تلفن و تلگراف نیپون، توافقی مدت‌دار با آژانس دفاعی ژاپن دارد تا مکالماتی را که برای شرکت‌های ژاپنی مورد توجه هستند، شنود کند. همچنین گفته می‌شود، ژاپنی‌ها در اتاق هتل‌ها، میکروفون کار می‌گذارند.(۳۷) بنا به گفته اسمیت، سفیر آمریکا که مدتی‌که معاون نماینده تجاری آمریکا بود به توکیو مسافرت کرده است: «طبقات و اتاق‌های خاصی در اکثر هتل‌های ژاپن همیشه میکروفون دارند. وقتی به ژاپن می‌رفتم آنها همیشه اصرار داشتند که من در طبقه هشتم یا نهم هتل خاصی اقامت کنم. بنابراین اگر می‌خواستیم درباره مطلب حساسی صحبت کنیم، همیشه باید از اتاق خارج می‌شدیم».(۳۸)

نیروهای مسلح میانمار (برمه) در رانگون یک مرکز نظارت الکترونیکی[1] را اداره می‌کنند. مدیریت اطلاعات نیروهای دفاعی در یک ایستگاه زمینی تانلین[2] در مخابرات بین‌المللی مستقر است که از جمله تماس‌های تلفنی، فاکس‌ها، پیام‌های الکترونیکی و دیگر موارد ارسال داده‌ها که از میان یکی از دروازه‌های سوئیچی (Switch gate) می‌گذرد، شنود می‌کند. این مدیریت، برای نظارت بر تلفن‌های ماهواره‌ای که با استفاده از ماهواره اینمارست[3] و دیگر سیستم‌های مخابرات راه دور ماهواره‌ای، اقدام به دور زدن مراکز مبادله می‌کنند، تکنولوژی خاصی را مستقر کرده است. تصور می‌شود استفاده از این تکنولوژی منجر به دستگیری حداقل چهار نفر از ناراضیان در رانگون[4] و ماندالای[5] شده باشد.(۳۹)

فرانسوی‌ها ظاهراً در صندلی‌های خطوط هوایی فرانسه و در اتاق هتل‌های پاریس میکروفون کار گذاشته و خطوط تلفن کشور را ضبط می‌کنند تا نقشه محصولات و مناقصه قراردادها را به‌دست آورند.(۴۰) بنا به گفته پیتر شوایتزر[6]، مدیر کل امنیت خارجی در سال ۱۹۸۸ یک تیم چهار نفره را به سیاتل فرستاد تا اقدام به شنود درباره داده‌های تست و مکالمات

1. Electronic Surveillance Centre
2. Tanlinne
3. Inmarsat
4. Roungone
5. Mondalay
6. Pitter Schouvitzer

یک تیم چهار نفره را به سیاتل فرستاد تا اقدام به شنود درباره داده‌های تست و مکالمات پرسنل در زمان آزمایش‌های پروازی هواپیمای جدید ۴۰۰ـ۷۴۷ بوئینگ نمایند. اطلاعات گردآوری شده درباره سیستم ناوبری کامپیوتری جدید به شرکت ایرباس کمک کرد تا سیستم مشابهی را روی A340 مستقر کند. «کمیسیون مستقل برای کنترل شنودهای امنیتی» گزارش داد که صد هزار خط تلفن هر ساله به‌طور غیرقانونی در فرانسه ضبط می‌شوند و مؤسسات دولتی در اکثر موارد استراق سمع، حضور دارند.(۴۱)

۹ـ۱ـ رمزگشایی پیام‌ها[1]

ممکن است پیام‌هایی که مؤسسات اطلاعاتی شنود کرده‌اند به خصوص آنهایی که متعلق به دولت‌های خارجی هستند، رمزگذاری شده باشند. بنابراین عملیات کسب اطلاعات از روی سیگنال‌ها نه تنها شامل دسترسی به پیام‌ها بلکه شامل رمزگشایی از آنهایی می‌باشد که به‌صورت مغشوش درآمده‌اند.(۴۲)

یکی از شناخته شده‌ترین تلاش‌ها برای شکستن رمز، درست قبل از ورود ایالات‌متحده به جنگ جهانی اول اتفاق افتاد. در ژانویه سال ۱۹۱۷ وزیر خارجه آلمان، به نام آرتور زیمرمان تلگرام رمزگذاری شده وست‌یونیون[2] را به سفارت آلمان در مکزیکوسیتی فرستاد. این پیام که شنود شده بود با موفقیت به‌دست رمزشکنان انگلیس در «اتاق شماره ۴۰» از رمز درآمد که خطاب به دولت مکزیک آمده بوده:(۴۳)

«ما قصد داریم جنگ نامحدود زیردریایی خود را در روز اول فوریه آغاز کنیم و تلاش خواهیم کرد تا به‌رغم این اتفاق، ایالات‌متحده را بی‌طرف نگاه داریم، در صورتی‌که در این مورد موفقیتی حاصل نشود بر مبنای ذیل به مکزیک پیشنهاد اتحاد خواهیم داد، با هم جنگ می‌کنیم، با هم صلح به‌دست می‌آوریم، به همراه آنها، یک پشتیبانی سخاوتمندانه مالی و این اذعان از طرف ما که مکزیک قرار است مناطق از دست داده خود در تگزاس، نیومکزیکو و

1. Deciphering the Messages
2. Artour Zeimerman

آریزونا را به‌دست آورد. جزئیات این پیمان برعهده شما است».[۴۴]

در اواخر فوریه، بریتانیایی‌ها یک کپی از پیام را به رئیس‌جمهور، وودرو ویلسون ارائه دادند. این پیام در اول ماه مارس در مطبوعات منتشر گشت و افکار عمومی آمریکا را بهت‌زده نمود.[۴۵] ویلسون که سه ماه قبل اعلام کرده بود هدایت کشور به درون جنگ، «جنایتی بر ضد تمدن است» در سخنرانی خود در کنگره در آوریل به تلگرام زیمرمان اشاره کرد و خواستار آن شد که کنگره بر ضد آلمان اعلان جنگ بدهد. آنها هم، همین کار را انجام دادند. ورود آمریکا به جنگ ورق را برگرداند و باعث شکست آلمان شد. دیویدکان، مورخ سرشناس و نویسنده «رمزشکنان»، نوشت: «حل یکی از پیام‌های رمز دشمن در اتاق شماره ۴۰، به ورود آمریکا به جنگ جهانی اول کمک کرد و به متفقین امکان داد تا برنده شوند. البته رمزگشایی واحدهای دیگر چنین پیامد عظیمی نداشته است.»[۴۶]

در طول جنگ جهانی دوم، موارد رمزگشایی پیام ژاپنی‌ها به‌دست آژانس امنیت ملی باعث پیروزی نیروی دریایی آمریکا در میدوی، دریای مرجان و جزایر سلیمان شد. رمزشکنان قادر بودند هشداری زود هنگام در مورد حمله پرل‌هاربر بدهند، اما کسی روی این پیام‌ها کاری انجام نداد تا اینکه زمان از دست رفت.[۴۷]

اما در کمتر از دو سال بعد، آژانس امنیت ملی برنامه پرواز دریا سالار ایزوروکو یاماماتو[1]، فرمانده کل نیروهای دریای ژاپن که این حمله را هدایت کرده بود، به‌دست آورد و جنگنده‌های آمریکایی، هواپیمای او را از روی آسمان منفجر کردند. در اقیانوس اطلس، رمزگشایی متفقین از پیام‌های آلمانی منجر به غرق‌شدن کشتی‌های آلمانی موسوم به U-boat گشت و به این ترتیب کشتی‌ها و زیردریایی‌های آمریکایی از حملات کشتی‌های در حال پرسه نجات یافتند و در نتیجه پیروزی در نبرد اقیانوس اطلس تضمین شد.[۴۸] آژانس امنیت ملی در پروژه دیگری به نام Verona از سال ۱۹۴۲ تا ۱۹۴۶ اقدام به شنود و رمزگشایی پیام‌های دیپلماتیک و اطلاعاتی شوروی کرد. این پروژه، شبکه جاسوسی گسترده شوروی در آمریکا را

---

1. Isoroko Yamamato

کشف کرد و منجر به دستگیری و محکومیت جولیوس[1] و اتل رزنبرگ[2] و هم دستان جاسوس آنها شد که اسراری را در مورد بمب اتمی و جزئیات هواپیماهای جت، رادار و موشک‌ها در اختیار شوروی قرار داده بودند.(۴۹)

البته با وجود تمام ادعاهایی که در خصوص دقت وسایل الکترونیک و رادارهای پیشرفته ناوهای آمریکایی می‌شد، یادآوری حادثه تأسف‌انگیز سرنگونی هواپیمای مسافربری ایرباس ایرانی بر فراز آب‌های خلیج‌فارس در سال ۱۳۶۷ و کشته شدن ۲۹۰ انسان بی‌گناه بر اثر آن، بسیار عبرت‌آموز است، چراکه آمریکا رسماً اعلام کرد که ناو وینسنز در محاسبات خود اشتباه کرده و هواپیماهای مسافری را یک جنگنده ایرانی فرض کرده که در حال شیرجه زدن به سمت ناو بوده است! یکی از چالش‌هایی که پیش روی دولت‌ها قرار دارد، این است که چگونه می‌توان اطلاعات به‌دست آمده از دستگاه‌های شنود و رمزگشاها را بدون از دست دادن توانمندی‌ها استفاده کرد.(۵۰) اگر از اطلاعات به‌دست آمده نتوان بهره برد، ارزش آن‌ها صفر خواهد بود. با وجود این، اگر اهداف قادر باشند از روی اقدامات انجام‌شده حدس بزنند که کدهای رمزشان شکسته شده است به احتمال قوی دست به تغییر آن کدها خواهند زد. تأثیر تغییر کد، از دست دادنِ منابع اطلاعاتی خواهد بود که در صورت حفظ شدن در درازمدت، می‌توانستند بسیار ارزشمند باشند.(۵۱)

چون اطلاع درباره تلاش‌هایی برای شکستن کدهای دولت خارجی برای آن دولت خارجی ارزش بسیاری دارد، این اطلاعات نامزد اصلی برای افشا شدنِ از طرف جاسوسان داخلی هستند.(۵۲)

۱۰ـ۱ـ آنالیز ترافیک[3]

پیام‌هایی که از طریق شبکه‌های مخابراتی، از جمله شبکه‌های تلفن و کامپیوتر ارسال می‌شوند

---

1. Joulious
2. Etel Rozenberg
3. Traffic Analysis

معمولاً دارای دو نوع اطلاعات هستند: محتویات پیام و اطلاعات برقراری ارتباط، اولی تعیین‌کننده دو طرف مکالمه است و می‌تواند شامل شماره تلفن طرف‌های تماس گیرنده و تماس گرفته شده، آدرس پست الکترونیکی یا قلمرو الکترونیکی و کدهای شناساگر کامپیوترها، دستگاه‌های ارتباطی و مؤسسات باشد. اطلاعات مربوط به برقراری ارتباط را می‌توان برای تعیین الگوهای ترافیک مورد استفاده قرار داد، یعنی اینکه چه کسی و در چه‌زمانی با چه کسی مشغول صحبت است. آنالیز ترافیک به فرد شنودکننده امکان می‌دهد تا روابط موجود و تغییرات انجام شده در کنش ارتباط را شناسایی کند. این امر حتی زمانی که محتویات به صورت مغشوش درآمد و قابل رمزگشایی نباشد، می‌تواند مفید واقع شود.

اطلاعات مربوط به برقراری ارتباط، شنود شده و هنگامی که نیاز کافی یا توجیهی برای ضبط گسترده مکالمات وجود نداشته باشد در تحقیقات و بازرسی‌های جنایی مورد استفاده قرار می‌گیرد. یک Pen register به مؤسسه مجری قانون امکان دسترسی به شماره‌های گرفته شده از روی تلفن سوژه را ممکن می‌سازد. روش «دام و تعقیب»[1] شماره‌هایی را که تلفن سوژه را می‌خواهند، اشغال کنند، مشخص می‌سازد. حکم دادگاه برای هر دو روش ضروری است، اما معیاری که تحت آن، این احکام صادر می‌شود به همان میزان احکام صادره برای شنود محتویات تماس، لازم‌الاجرا نیستند.(۵۳)

با وجودی‌که اکثر موارد اجرایی با روش‌های فوق بر ضد مکالمات تلفنی به کار گرفته می‌شوند، اما موارد انگشت‌شماری در ترافیک شبکه‌های کامپیوتری مورد استفاده قرار گرفته‌اند.(۵۴)

۱۱ـ۱ـ ردیابی محل[2]

سیستم‌های تلفن همراه را می‌توان برای ردیابی محل تماس‌گیرنده و نیز شماره تلفن ارتباطات مورد استفاده قرار داد. حتی هنگامی‌که تلفن مورد استفاده قرار نمی‌گیرد، محل آنرا می‌توان

1. Trap and Trace
2. Location Tracking

ردگیری کرد به شرطی‌که مشخص باشد و علت آن این است که تلفن، سیگنال‌هایی ساطع می‌کند که به‌وسیله ایستگاه‌های مبنا دریافت می‌شوند. در نامحتمل‌ترین حالت، محل مورد نظر را می‌توان محدود به یک منطقه جغرافیایی کرد که ایستگاه مبنا آنجا را پوشش می‌دهد. سیستم‌هایی با دقت بیشتر، در حال توسعه و تکمیل هستند تا ملزومات مورد توجه سرویس‌های ۹۱۱ اضطراری و اجرای قانون را برآورده سازند.

ردیابی محل، باعث ایجاد نگرانی‌هایی در مورد حفظ حریم خصوصی شده است. در آمریکا گروه‌هایی درخواست کرده‌اند تا معیار اعطای حکم دادگاه به سطح افرادی رسانده شود که به‌دنبال محتویات تماس هستند، یعنی مستلزم دارابودن دلیل احتمالی یک فعالیت جنایی است.

در اکتبر سال ۱۹۹۷، مجله Fortune گزارش داد که شرکت Personal، شرکت وابسته NTT که «سیستم هندی فون شخصی ژاپن» را اداره می‌کند، مشغول آزمایش با یک وب سایت بوده که می‌تواند به هر کس اجازه دهد تا محل یک تلفن را (و شاید فردی که آنرا در دست دارد) با تایپ کردن شماره تلفن پیدا کند. این مجله که مراجعه‌ای به این سایت داشت (که تا آن موقع حالت عمومی پیدا نکرده بود) گزارش داد که این سایت، مختصات دقیق نقشه تا طبقه ساختمانی که تلفن مورد نظر در آن مستقر است را ارائه می‌دهد. این دقت به این علت امکان‌پذیر شده بود که سیستم هندی فون شخصی در مقایسه با سیستم‌های سلولی، یک سیستم کم‌قدرت محسوب می‌شود، بنابراین ایستگاه‌های مبنا (تقویت‌کننده‌ها) بسیار نزدیک یکدیگر قرار می‌گیرند. این وب سایت سؤالاتی جدی در مورد حریم خصوصی مطرح می‌کند.[۵۵]

۱۲ــ۱ــ کلاهبرداری مخابراتی[۱]

این روش به چندین صورت امکان‌پذیر است، از جمله telabuse (بد استفاده کردن خودی‌ها)، کلاهبرداری راه دور و کلاهبرداری سلولی. در اینجا آشکالی مورد توجه ویژه قرار دارند که فرد خاطی اقدام به تحمیل هزینه به یک حساب می‌کند به طوری‌که هزینه‌های سرویس سرقت

1. Telecommunications Fraud

شده، به حساب فاش شده تحمیل می‌شود. از زاویه دید جنگ اطلاعاتی، فرد خاطی به یک منبع اطلاعاتی دست پیدا می‌کند (در این مورد، یک خط تلفن) و به خرج صاحب حساب یا ارائه‌دهنده خدمات از آن بهره می‌برد.

کلاهبرداری مخابراتی امری متداول و عمدتاً پرهزینه است. حدود ۱۴٪ پاسخ‌دهندگان به نظرسنجی سال ۱۹۹۸ FBI و CSI موسوم به «نظرسنجی امنیت و جرائم کامپیوتری» گزارش دادند که در طول سال گذشته مواردی از کلاهبرداری مخابراتی را کشف کرده‌اند. یک شرکت به تنهایی گزارشی از ۱۵ میلیون دلار خسارت ارائه داد.(۵۶)

شرکت «مشاوران مخابراتی» در گزارشی دو جلدی در خصوص موارد کلاهبرداری راه دور و سوءاستفاده از خودی‌ها که در سال ۱۹۹۲ منتشر شد، تخمین زد که هزینه کلی کلاهبرداری مخابراتی در آمریکا حدود ۸/۹ میلیارد دلار باشد.(۵۷) سوءاستفاده خودی‌ها بیش از نیمی از هزینه‌ها (یعنی ۵/۲ میلیارد دلار) را به خود اختصاص داد. سرویس‌های راه دور سرقتی با ۱/۸ میلیارد دلار در مقام دوم این گروه قرار گرفت. در انگلستان گفته می‌شود کلاهبرداری مخابراتی بیش از ۳۰۰ میلیون دلار در سال برای شرکت‌های تلفن و مشتریانش هزینه دارد.(۵۸) خسارت‌های برآورد شده در آلمان نیز مشابه است. بنا بر اعلام پیتر هاوث[1]، برخی از تخمین‌ها در مورد کلاهبرداری مخابراتی جهانی، این خسارت‌ها را به ۳۰ میلیارد دلار در سال می‌رساند.(۵۹)

جو هوروات[2]، مدیر منطقه‌ای شعبه مدیریت خطرات در شرکت South western Bell Telephone در سال ۱۹۹۰ گزارش داد که کلاهبرداری تلفنی به مدت ۲۰ سال این صنعت را دچار آفت کرده است.(۶۰) موارد اولیه شامل دانشجویانی بود که از شماره کارت‌های اعتباری تقلبی استفاده می‌کردند تا با خانواده و دوستان خود تماس بگیرند. «در آن روزها برای تماس گرفتن، مجبور بودید از طریق یک اپراتور متصل شوید که خود، هیچ راهی برای ارزیابی این نکته نداشت که آیا شماره کد ساده‌ای که مورد استفاده قرار گرفته معتبر است یا خیر».(۶۱)

1. Peter Hoath
2. Joe Horvat

۱۳ـ۱ـ جعبه‌های آبی[1]

تصور می‌شود اولین مورد از کلاهبرداری تلفن‌های راه دور در سال ۱۹۶۱ به‌وقوع پیوسته باشد، یعنی زمانی‌که شرکت Bell Telephone فردی را دستگیر کرد که از یک جعبهٔ آبی استفاده می‌کرد تا تماس‌های رایگان راه دور را برقرار کند. در دهه ۶۰ و اوایل دهه ۷۰ میلادی تمام کیوسک‌های تماس راه دور نسبت به سیگنالی با فرکانس ۲۶۰۰ هرتز حساس بودند.(۶۲) جعبه‌های آبی با شبیه‌سازی ۲۶۰۰ تن هرتزی و دیگر تن‌های مورد نیاز برای آغاز سرویس‌هایی خاص، کار می‌کردند. از آنجا که این سیگنال‌ها برروی همان کانال صدای انسان انتقال می‌یافتند، تنها چیزی که مورد نیاز بود روشی برای وارد کردن سیگنال بر روی خط بود. برای این کار، فرستنده‌ای در یک جعبه به‌طور آکوستیک[2] به یک تلفن یا با کمک سیم به یک خط تلفن متصل می‌شد.(۶۳) ساخت یک جعبه آبی، نیازمند تخیلات زیادی نبود، چراکه Ma Bell خصوصیات آنرا در مقاله‌ای به سال ۱۹۵۴ در مجله فنی Bell System و در مقاله‌ای دیگر در نوامبر سال ۱۹۶۰ منتشر کرده و به این ترتیب جزئیات سیستم تن شرکت Bell را افشا کرده بود. علاوه بر جعبه‌های آبی، جعبه‌های قرمز هم وجود داشتند که شبیه‌ساز تن‌هایی بودند که سکه‌های انداخته شده در یک تلفن را می‌شمردند و جعبه‌های سیاه که اجازه می‌دادند تا تماس‌های راه دور بدون صدور صورت هزینه دریافت شوند. این جعبه‌ها در نهایت از سیستم‌های پیشرفته مخابراتی شکست خوردند.(۶۴)

۱۴ـ۱ـ PBX و کلاهبرداری مرتبط

متقلبان امروزی روش‌های دیگری را برای سرقت سرویس تلفن آموخته‌اند. یکی از روش‌های متداول شامل دسترسی به مرکز مبادله خصوصی شاخه‌ها[3] (PBX) در شرکت و سپس استفاده از توابع آن برای برقراری تماس‌های راه دور به خرج شرکت است.(۶۵) یکی از دانشگاه‌های

---

1. Blue Boxes
2. Acoustically
3. Private Branch Exchange (PBX)

آمریکا، زمانی متوجه این روش شد که صورت‌حساب تلفن‌هایش را که ۲۰۰ هزار دلار شده بود به‌جای پاکت نامه در یک جعبه دریافت کرد.[۶۶] یکی از سازندگان کامپیوتر در عرض یک ماه، ۳۰۰ هزار دلار ضرر کرد. دیگری در یک روز آخر هفته ۷۰۰ هزار دلار به‌علت حمله به ۴۳ مورد از PBXهای خود ضرر کرد.[۶۷] در مورد دیگری نیز هکرها دست به عملیاتی زدند که در عرض یک تعطیلات چهار روزه بیش از ۱/۴ میلیون دلار هزینه به بار آورد.[۶۸]

کلاهبرداری مخابراتی به چند دلیل برای خلافکارها جالب است. اول اینکه، خطر دستگیر شدن بسیار اندک است، چرا که بعید به‌نظر می‌رسد که، جرائم به‌خصوص آنهایی که از دور انجام می‌شوند، به این آسانی شناسایی و ردگیری شوند. یک Phreaker می‌تواند از طریق مدارهای بین‌المللی، شبکه‌های خصوصی یا حاملان دارای ارتباط متقابل، مسیر تماس را تغییر دهد. دوم، برای برخی از انواع حملات، نیاز به هیچ‌گونه تجهیزات ویژه‌ای وجود ندارد. سوم، در تماس‌های تلفنی پول وجود دارد. کلاهبردارها به کرات سرویس‌های راه دور سرقتی را به اشخاص ثالث می‌فروشند و باعث تنزل نرخ‌های استاندارد می‌شوند.[۶۹] در یک مورد، جوانی ۲۷ ساله در آرژانتین به خطوط تلفن خصوصی آژانس خبری رویترز دست پیدا کرد و سرویس‌های فاکس و تلفن Callback را به خرج شرکت به فروش رساند. وی همین کار را برای دفتر آرژانتینی شرکت اروپایی نستله انجام داد. برآورد شده که کل خسارت‌ها برای هر دو شرکت نزدیک به $\frac{1}{4}$ میلیون دلار باشد.[۷۰]

این افراد در اغلب موارد قادرند با شکستن کدهای ساده وارد سیستم‌های مخابراتی شوند. بنا به اعلام شرکت Central & East European Crim Scope مجرمین عرب‌زبان، کدی را در تلفن‌های کارتی مقدونیه شکستند و توانستند تماس‌های راه دور را به رایگان برقرار سازند. ابتدا آنها شماره یک سوئیچ برد را می‌گیرند. سپس هنگامی که پیام ضبط شده شروع به پخش می‌کند، آنها یک ۹ را که بعد از آن کد مخفی ۴ رقمی قرار دارد، می‌گیرند. در بسیاری از موارد کد پیش گزیده ۱۱۱۱ است. هکرها از این تکنیک برای ورود به تلفن‌های وزارت خارجه مقدونیه استفاده کردند.[۷۱]

مهندسی اجتماعی، ابزار دیگری است که برای سرقت سرویس‌های تلفن مورد استفاده قرار می‌گیرد. یک جوان ۲۱ ساله فرانسوی به نام آنتونی زبورالسکی[1] از طریق کسب نام یکی از نمایندگان FBI در فرانسه از سفارت آمریکا در پاریس ۲۵۰ هزار دلار تماس تلفنی به هزینه FBI انجام داد. سپس وی که خود را جای آن شخص جا زده بود به دفتر FBI در واشنگتن زنگ زد و درخواست اطلاعاتی در مورد نحوه اتصال به سیستم کنفرانس FBI را کرد. وی از این اطلاعات برای گپ زدن با دوستان خود در سرتاسر دنیا و در دوره چند ماهه در سال ۱۹۹۴ استفاده کرد. او در فوریه سال ۱۹۹۷، ۸۸۵۰ دلار جریمه شد، حکم زندان تعلیقی ۱۸ ماهه دریافت کرد و به مدت ۲ سال به‌علت کلاهبرداری در آزادی تحت نظر قرار گرفت. مقامات دادگستری گزارش دادند که وی برای نوشتن کتابی در مورد کار خود با ناشری قرارداد بسته است.(۷۲)

کوین میتنیک[2] به‌دلیل مهارت‌هایی که در امر مهندسی اجتماعی داشت، قبلاً مورد نظر قرار گرفته بود. با صدای آرامش‌بخش که ایجاد کننده اعتماد بر شکاک‌ترین حافظان اسم رمزها بود، غلبه می‌کرد. او با دوستش راسکو[3] که خود را جای یک ناظر عصبانی جا می‌زد با اداره مخابراتی یک شرکت تماس می‌گرفتند و درخواست می‌کردند تا در مورد اینکه چرا شماره خاصی کار نمی‌کند، اطلاعاتی به آنها بدهند. آنها بی‌تردید هر چیزی را که لازم داشتند تا بتوانند از آن شماره به نحو مقتضی استفاده کنند به‌دست می‌آوردند. راسکو حتی از اطلاعات درباره افرادی که با آنها صحبت کرده بود، یک بانک اطلاعاتی تشکیل داده و یادداشت گذاشته بود که آیا آنها افراد تازه‌کاری هستند یا باتجربه، مطلع‌اند یا بی‌خیال، همکاری می‌کنند یا خیر و همچنین سرگرمی‌های شخصی، اسم کودکان، سن، ورزش‌های مورد علاقه و محل‌های تعطیلات آنها را ثبت کرده بود. قربانیان این افراد می‌توانند علاوه بر پول، خسارات دیگری نیز ببینند.(۷۳)

1. Anthony Zboralski
2. Coine Mitnice
3. Rasco

۱۵ـ۱ـ کلاهبرداری در پست صوتی (Voice Mail)

هکرها به سیستم‌های پست صوتی نیز دست یافته‌اند. در ۹ فوریه سال ۱۹۸۹، رئیس شرکت املاک و مستغلات ایلینویز به سرویس مخفی آمریکا تلفن زد تا گزارش دهد که کامپیوتر پست صوتی شرکت او هک شده است. آن تماس در نهایت، منجر به محکومیت خانم لسلی لین دوچت[1] شد، چراکه به‌عنوان رئیس طرح کلاهبرداری کامپیوتری از پست صوتی، وارد عمل شده و ۴۸۱ کد دسترسی به‌دست آورده بود. این کدهای دسترسی، شامل شماره‌های کارت اعتباری، شماره‌های کارت تماس تلفنی، کدهای تماس راه دور PBX و اسم رمزهای کامپیوتری بودند. او این کدها و دیگر موارد را در صندوق‌های پست صوتی به ۱۲۵ هکر فروخته بود. خسارت‌های تخمینی ۵۹۵۹۴۱ دلار می‌شدند که شامل بلیط هواپیما و اقامت خریداری شده با کارت‌های اعتباری سرقتی بود.(۷۴)

شرکت‌هایی که سیستم‌های پست صوتی آنها را بتوان به خطر انداخت نه تنها در برابر کلاهبرداری بلکه در برابر جاسوسی نیز آسیب‌پذیرند. در سال ۱۹۹۷، پسر ۱۵ ساله‌ای که خود را «آقای هیچ‌کس»[2] می‌نامید سیستم پست صوتی شرکت خدمات ارتباطات آن‌لاین نت کام را شکست. وی علاوه بر تماس‌های راه دور از سیستم پست صوتی برای استراق سمع کارهای شرکت استفاده می‌کرد.(۷۵)

هکرها تلاش کردند تا از روش باجگیری برای به‌دست آوردن صندوق‌های پست صوتی امن استفاده کنند. در موردی که در کالیفرنیا ثبت شده، یک هکر قول خود را به اثبات رساند و امتیازات کاربران خاص در سیستم را به‌دست آورد. مدیر سیستم مجبور بود درون سیستم خود را هک کند تا دوباره کنترل را در دست بگیرد، اما مصالحه با هکرها می‌تواند منجر به پیامدهای حاد و دردسرسازی شود.(۷۶)

در رویداد دیگری، یک هکر ۱۵ ساله که خود را Cellular Phantom می‌نامید. یک تبریک

---

1. Leslie Lynne Docette
2. Mr. Nobody

کریسمس بر روی سیستمی نصب کرد که تحت اداره شرکت Voice Mail inc بود. این شرکت در اوهایو به شرکت‌های محلی، صندوق پستی‌های صوتی اجاره می‌دهد. این پیام که در اواخر دسامبر سال ۱۹۸۷ برروی سیستم قرار گرفت به تماس گیرنده‌ها در تمامی خطوط این شرکت، همراه با جریانی از ناسزاها، تبریک می‌گفت. این هکر، خواهان استفاده نامحدود از ۵ تا ۱۰ صندوق پست صوتی بود و تهدید می‌کرد که اگر درخواستش را قبول نکنند، سیستم را نابود خواهد کرد. سرانجام این شرکت به‌وسیله موارد متعدد هک شدن از کسب و کار باز ماند.(۷۷)

بین ۲۷ ژانویه سال ۱۹۹۵ و ۱۸ آوریل ۱۹۹۶، ۳۲ هکر در انگلستان بازداشت شدند که علت عمده آن هک کردن سیستم‌های پست صوتی و PBX بود. اکثریت آنها (۵۴٪) قصد آسیب رساندن نداشتند، ۱۳ نفر (۴۱٪) از سیستم سوءاستفاده می‌کردند تا تماس‌های تلفنی رایگانی برقرار سازند و ۴ نفر (۱۳٪) سیستم‌های پست صوتی را دستکاری کردند تا برای دوستان خود پیام بگذارند. ۴۶٪ باقیمانده نیز قصد داشتند تا از کار خود سود مادی ببرند. ۵ نفر، از سیستم‌ها سوءاستفاده کردند تا تماس‌هایی را بر روی خطوط ویژه راه‌اندازی کنند و درآمدی از این راه حاصل نمایند. ۵ نفر دیگر هم در تکثیر قاچاق نرم‌افزار درگیر بودند. ۲ نفر در عملیات فروش تماس و ۲ نفر هم در سرقت کارت اعتباری دخیل شده بودند. خلافکار آخری به عمد هزینه‌های تماس را روی خط یکی از کارفرمایان سابق خود می‌فرستاد. نیمی از هکرها دانش‌آموزانی بودند که سنشان از ۱۴ تا ۲۲ سال متغیر بود، حدود $\frac{۱}{۳}$ از آنها بیکار و سنشان بین ۱۸ تا ۳۵ سال بود و ۱۶٪ باقیمانده از سن ۱۸ تا ۳۱ سال و شاغل بودند. متوسط سن همه آنها ۲۱ سال بود و فقط یک نفر از آنها زن بود.(۷۸)

۱۶ـ۱ـ کلاهبرداری از کارت‌های تلفن

کلاهبرداری از کارت‌های تلفن، شامل استفاده غیرمجاز[1] از کارت‌های تماس تلفنی می‌باشد. در

---

1. Unaut Horized use

برخی موارد سارقان شماره کارت‌های دزدی را روی بولتن بردها منتشر کرده، یا آنها را به اشخاص ثالثی می‌فروشند.

عملیات Sundevil، حمله‌ای سرتاسری به هکرهای کامپیوتری که توسط دفتر دادستان کل آمریکا در فونیکس آریزونا انجام شد، کلاهبرداری کارت‌های اعتباری و کارت‌های تلفنی را هدف گرفته بود. در ماه مه سال ۱۹۹۰ بیانیه‌ای مطبوعاتی، آشکار ساخت که ۱۵۰ نفر از مأموران سرویس مخفی در ۱۲ شهر آمریکا، ۲۷ حکم تفتیش را عملی نموده و ۳ نفر را هم بازداشت کرده‌اند. حدود ۲۵ دستگاه از ۴۲ دستگاه کامپیوتر توقیف شده برای راه‌اندازی بولتن بردهای کامپیوتری زیرزمینی مورد استفاده قرار می‌گرفت تا هکرها در آنجا کارت‌های اعتباری دزدی را مبادله کنند. خسارت‌های تخمین زده که بر شرکت‌های مخابراتی تحمیل شده بودند به تنهایی به میلیون‌ها دلار می‌رسید. این عملیات با هدف ارسال پیامی قاطع به محافل هکری بود: هک کردن‌های غیرقانونی از نظر دور نخواهد ماند.(۷۹) در سال ۱۹۹۴، ماکس لوران[1] از مایورکای[2] اسپانیا به‌علت کمک به هماهنگی یکی از بزرگ‌ترین کلاهبرداری‌های کارت تلفن تا آن زمان، بازداشت شد. مقامات تخمین می‌زدند که شبکه دزدان در آمریکا، ۱۴۰ هزار شماره کارت را به سرقت برده و به‌طور متوسط هزار دلار در هر کارت هزینه غیرمجاز ایجاد کرده‌اند. کل هزینه، ۱۴۰ میلیون دلار بود. شماره کارت‌ها توسط شبکه‌ای از عرضه‌کننده‌ها به‌دست می‌آمد که برخی از آنها برای شرکت‌های تلفن کار می‌کردند. یکی از عرضه‌کنندگان متهم به نام ایوی جیمز، معروف بود که به‌عنوان مهندس سوئیچ در یکی از مراکز سوئیچینگ[3] MCI در کارولینای شمالی کار می‌کند. وی متهم به سرقت ۱۰۰ هزار شماره کارت و فروش آنها در سرتاسر اروپا و آمریکا بود.(۸۰)

خلافکارها میلیون‌ها دلار از شرکت‌های تلفن راه دور با کارت‌های تلفن از پیش پرداخت شده به سرقت برده‌اند. در یکی از سناریوهای معمولی، آنها یک شرکت کارت تلفن تأسیس

---

1. Max Lourane　　2 Mayorka
3. Switching Centre

می‌کنند. این شرکت با یک عرضه کننده خدمات راه دور قرارداد می‌بندد و هزاران کارت را به فروش می‌رساند، اما پولی را به حامل نمی‌پردازد. در موردی که گفته می‌شد اولین مورد در نوع خود است، ۵ نفر در نیویورک به جرم استفاده از تماس سه طرفه برای سرقت کارت‌های تلفنی دستگیر شدند.[۸۱] بنا بر اسناد فدرال، این گروه تماس‌هایی را برای تلفن‌های سکه‌ای در فرودگاه‌ها ایجاد می‌کردند. وقتی افراد می‌خواستند از تلفن‌ها استفاده کنند به آنها جواب می‌دادند که آنها صدای چیزی را می‌شنیدند که شبیه تن شماره‌گیری بوده و از طریق تماس کنفرانسی تلفن فعال می‌شد. افراد استراق سمع کننده این تن‌ها را یادداشت می‌کردند و آنها را با استفاده از یک ضبط‌کننده شماره تماس، تبدیل به اعداد می‌کردند. حتی اگر تماس‌گیرنده، گوشی را می‌گذاشت، نوار به مدت ۱۵ ثانیه فعال می‌ماند. بازرسان اظهار می‌داشتند که صدها شماره کارت تلفن از مسافران فرودگاه در آتلانتا، شیکاگو، دنور، و هیوستن به سرقت رفته است.[۸۲]

۱۷ـ۱ـ تلفن‌های شبیه‌سازی شده[۱] و کلاهبرداری سلولی[۲]

کلاهبرداری سلولی، شامل استفاده غیرمجاز و شیادانه از خدمات تلفن همراه است. قسمت اعظم این خسارت از فرآیند Cloning (شبیه‌سازی) حاصل می‌شود، یعنی تولید تلفن‌هایی با همان شماره‌هایی که تلفن‌های اختصاص یافته به مشتریان قانونی دارند. هنگامی که تماسی روی تلفن شبیه‌سازی شده قرار می‌گیرد، صورت‌حساب آن برای صاحب تلفن اصلی صادر می‌شود، اما وقتی تماس شیادانه شناسایی می‌شود، هزینه‌ها از حساب مشتری حذف شده و به‌عنوان خسارت‌هایی از طرف شرکت تلفن جذب می‌گردند.[۸۳]

تلفن‌های سلولی آنالوگ با کمک اسکنر ESN/MIN شبیه‌سازی می‌شوند. این سیستم شماره سریال الکترونیک (ESN) یک تلفن و شماره شناسایی موبایل (MIN) آن در هنگامی‌که این شماره‌ها در طول برقراری تماس ارسال می‌شوند را برمی‌دارد. یک اسکنر پیشرفته‌تر به نام

---

1. Cloned Phones

2 Cellular Fraud

«جعبه رهگیر داده‌های دیجیتالی»[1] به سراغ کد امنیتی PIN می‌رود، سپس مقادیر سرقت شده در یک تلفن سلولی دیگر برنامه‌ریزی می‌شوند تا یک تلفن شبیه‌سازی شده تولید گردد و هزینه‌های تماس به حساب فرد قربانی واریز شود.(۸۴)

تبهکاران در زمینه تلفن‌های همراه خیلی توجه نمی‌کنند که تلفن چه کسی شبیه‌سازی می‌شود، بنابراین آنها از هر جفت شماره ESN و MIN که اسکنرشان به‌دست می‌آورد، استفاده می‌کنند. ممکن است آنها عملیات استراق سمع خود را در یک پل روگذر بزرگراهی یا در یک اتاق هتل در نزدیکی یک سرعت‌گیر بزرگراه یعنی جایی‌که ترافیک سنگین است، انجام دهند. به این ترتیب می‌توانند محصول خوبی از شماره‌ها را از روی هوا برداشت کنند.(۸۵)

کار شبیه‌سازی، مشکلی است که عمدتاً متوجه تلفن‌های سلولی آنالوگ[2] بوده، چراکه این نوع تلفن‌ها برای حفاظت از پیام‌های خود (که در هوا در تردد هستند) در برابر شنود دیگران از رمزگذاری استفاده نمی‌کنند. اما تلفن‌های دیجیتالی معمولاً مصونیت داشته‌اند. تلفن‌های شبیه‌سازی شده در بازار سیاه به گانگسترها، متخصصان مواد و دیگر مجرمانی فروخته می‌شوند که از آنها برای فرار از دست پلیس استفاده می‌کنند. در یکی از موارد که کارتل مواد مخدر کلمبیا درگیر بود، مقامات اداره مبارزه با مواد مخدر در آمریکا تعداد نامتعارفی از تماس‌ها به کلمبیا را در صورت‌حساب‌های تلفنی خود کشف کردند. مأموران مخفی این کارتل، شماره تلفن‌های اداره مبارزه با موّادمخدر را شبیه‌سازی کرده بودند.(۸۶)

در اغلب موارد، تلفن شبیه‌سازی شده یک‌بار مورد استفاده قرار گرفته و سپس دور انداخته می‌شود. مدیر ارشد کارتل Cali می‌تواند در روز تا ۳۵ تلفن همراه مختلف را مورد استفاده قرار دهد. برخی از تلفن‌های شبیه‌سازی شده که به نام تلفن‌های مادام‌العمر مشهورند، حداکثر ۹۹ شماره سرقتی را در خود نگاه می‌دارند. می‌توان شماره‌های جدید را از روی یک شماره‌گیر دکمه‌ای به درون تلفن برنامه‌ریزی کرد و بنابراین این امکان را به کاربر می‌دهد تا برای هر تماس از یک شماره شبیه‌سازی شده متفاوت، استفاده کند.(۸۷)

---

1. Digital Data Interceptor Box

2 Analog Cell Phones

تلفن‌های شبیه‌سازی شده در عملیات‌های موسوم به «فروش تماس»[1] مورد استفاده قرار می‌گیرند. خلافکارها در مناطق فقیر و مهاجرنشین فروشگاهی را راه‌اندازی می‌کنند و در آنجا برای افرادی که می‌خواهند به اعضای خانواده خود در دوردست‌ها تلفن بزنند، تماس‌های راه دور ارزان قیمت می‌فروشند. به این ترتیب آنها پولی را به جیب می‌زنند که می‌باید به جیب شرکت ارائه‌دهنده آن خدمات می‌رفت. در پدیده‌ای که بزرگ‌ترین سرقت تاریخ آمریکا در آن زمان نامیده شد، دو نفر از بروکلین در ماه ژوئیه سال ۱۹۹۶ به جرم سرقت ۸۰ هزار شماره تلفن همراه از افرادی در کانتیکات، نیوجرسی، نیویورک، پنسیلوانیا دستگیر شدند. این شماره‌ها در بازار سیاه ۸۰ میلیون دلار ارزش داشت.[۸۸]

در ۱۰ نوامبر سال ۱۹۹۷سنای آمریکا، لایحه‌ای را تصویب کرد و تملک یا فروش دستگاه‌های مورد استفاده برای شبیه‌سازی تلفن‌های همراه را جرم اعلام کرد. مدل مشابهی از این لایحه در مجلس نمایندگان در جریان بود.

پیجرهای شبیه‌سازی شده[2] با فرآیندی مشابه شبیه‌سازی تلفن‌ها، تولید می‌شوند. در این حالت، کدی که شناساگر پیجر است از هوا گرفته شده و در پیجر دیگری برنامه‌ریزی می‌شود. سپس پیجر شبیه‌سازی شده پیام‌هایی را که به آن کد ارسال می‌گردند، دریافت می‌کند.[۸۹]

نظارت بر شبکه‌های کامپیوتری، هم در جنگ تدافعی اطلاعات[3] و هم در جنگ تهاجمی اطلاعات[4] دارای کاربرد است. در بعد تهاجمی، متجاوزان کامپیوتری اقدام به استراق سمع در پیام‌های شبکه می‌کنند و در بعد تدافعی هم که به‌طور مفصل مورد بحث و بررسی قرار خواهد گرفت، مدیران سیستم فعالیت متجاوزان وخودی‌هایی را که از شبکه خود سوءاستفاده می‌کنند، ردگیری می‌کنند.

---

1. Call Sell Operations
2. Cloned Pagers
3. Defensive Information Warfare
4. Offensive Information Warfare

۱۸ـ۱ـ Sniffers

قسمت اعظم ترافیک شبکه‌های کامپیوتری در برابر شنود Snifferها، آسیب‌پذیرند. اینها برنامه‌هایی هستند که در بعضی از کامپیوترهای متصل شده به شبکه مستقر می‌شوند. Sniffer، پیام‌ها را هنگامی‌که در شبکه انتقال داده می‌شوند، می‌گیرند و پیام‌هایی را که مورد توجه‌شان است برای پیگیری بعدی در یک Log File ذخیره می‌کنند. چون پیام‌ها به‌صورت بلوک‌هایی از داده‌ها به نام «بسته» (Packet) روی شبکه در تردد هستند، این Snifferها به نام Packet Sniffer نیز معروفند. می‌توان یک پیام واحد پست الکترونیکی یا صفحه وب را به چند بسته تقسیم کرد و سپس به شبکه ارسال نمود. این بسته‌ها در محل دریافت از نو کنار هم گذاشته می‌شوند تا پیام مورد نظر تکمیل شود.

در ابتدایی‌ترین حالت، Sniffer می‌تواند بسته‌هایی را که در کامپیوتر خود در تردد است، بگیرد. اگر آن میزبان یک مسیریاب (Router) یا دستگاه دروازه (gate Way) باشد که دو یا چند شبکه را به هم متصل می‌کند، جریان ترافیک از میان آن میزبان قابل توجه خواهد بود.[۹۰]

Sniffer مستقر بر روی هر کامپیوتر که به شبکه متصل است با برخی از تکنولوژی‌های شبکه، مانند token ring، می‌تواند تمام پیام‌هایی را که از درون شبکه در جریان هستند (صرفنظر از مقصدی که دارند) بخواند. علت آن، این است که پیام‌ها روی شبکه منتشر می‌گردند و به هر کامپیوتر موجود در آن شبکه اجازه می‌دهند تا آنها را بگیرند. در جایی‌که یک دستگاه را می‌توان طوری پیکره‌بندی کرد تا از پیام‌هایی که خطاب به آن نیست، چشم‌پوشی کند، می‌توان آنرا طوری تنظیم نمود که در حالت بی‌نظمی قرار گرفته و بر تمام ترافیک موجود نظارت داشته باشد. اما کامپیوتر نمی‌تواند ترافیک موجود بر روی شبکه‌های دیگر را بخواند. مثلاً Sniffer مستقر بر روی یک شبکه محلی (Local area) نمی‌تواند ترافیک موجود بر روی شبکه محلی دیگر را شنود کند. هکرها از Pocket Sniffer برای به‌دست آوردن نام کاربری و اسم رمز استفاده می‌کنند، همچنین مورد استفاده مدیران شبکه نیز می‌باشد تا مانع از ورود هکرها شوند.[۹۱]

۱۹ـ۱ـ نظارت بر نواخته شدن کلیدها[1]

نظارت بر نواخته شدن کلیدها، عبارت است از رهگیری هر یک از کلیدهای زده شده در هنگامی‌که فرد چیزی را تایپ می‌کند. این روش به کرات مورد استفاده مدیران شبکه و بازرسان قرار می‌گیرد تا متجاوزان ردگیری شوند.

۲۰ـ۱ـ مراقبت محیطی[2]

انواع مختلفی از حسگرها برای گردآوری اطلاعات از محیطزیست فیزیکی وجود دارند، از جمله سیستم‌های تصویرسازی و دوربین‌ها. بخش‌های زیر به توصیف برخی از این حسگرها می‌پردازند.

۲۱ـ۱ـ دوربین و ویدئو

دوربین‌های ویدئویی در بانک‌ها، فروشگاه‌ها، فرودگاه‌ها، ساختمان‌های اداری، پارکینگ‌ها و دیگر مناطق مورد استفاده قرار می‌گیرند، تا جلوی سارقان، دزدان فروشگاه‌ها، خرابکارها و دیگر انواع خلافکارها را بگیرند. با وجودی‌که هدف از نظارت و مراقبت در چنین محیط‌هایی دفاع در برابر جرم است، می‌توان آنرا نوعی جنگ تهاجمی اطلاعات نامید که بر ضد خلافکاری آینده انجام می‌شود. هدف عبارت است از کسب اطلاعات درباره رفتار آنها.(۹۲)

انتظار می‌رود بازار سیستم‌های نظارت ویدئویی با کاهش قیمت‌ها و افزایش کیفیت، منفجر شده و اکثر گروه‌ها و مؤسسات اقدام به نصب دوربین‌های بیرونی در مناطقی که از نظر کارهای خلاف پرخطر هستند، نمایند.(۹۳)

در انگلستان یعنی جایی‌که بیش از ۳۰۰ شهر اقدام به نصب سیستم‌های مراقبتی ویدئویی در مناطق عمومی کرده‌اند، شخصی از روی نوارهای مراقبت که از شرکت‌های دولتی و امنیتی

---

1. Keystroke Monitoring
2. Environment Surveillance

خریداری کرده بود، فیلمی به نام «دستگیری در حین ارتکاب» را ساخت. این فیلم مردی را در هنگام اقدامات جنسی و نیز در هنگام ارتکاب جرائمی دیگر نشان می‌داد. گزارشی از کلایو وریس[1] در مرکز جرم‌شناسی دانشگاه هال و گری‌آرمسترانگ[2] ارزش این برنامه را زیر سؤال برد. محققان ۶۰۰ ساعت را صرف تماشای اپراتورهایی کردند که در سه مکان مخفی با ۱۴۸ دوربین به کار نظارت مشغول هستند. آنها گزارش دادند که از ۹۰۰ نفر مورد توجه، حداقل ۵۰٪ «بی‌هیچ دلیل خاصی» تحت نظر قرار گرفتند و به‌علت اینکه اپراتورهای دوربین «نسبت به جوانان مذکر و به‌خصوص جوانان سیاه‌پوست طرز تلقی منفی داشتند»، انتخاب شدند. تنها ۲۰ نفر از این ۹۰۰ نفر بازداشت شدند. مقامات به این جمع‌بندی رسیدند که سیستم می‌تواند تبدیل به «ابزار بی‌عدالتی» شود، مگر اینکه با دقت بیشتری تحت کنترل قرار گیرد.(۹۴)

همچنین در انگلستان، شرکت بریتیش تله کام گزارش داد که نظارت‌های ویدئویی ۲۴ ساعته عملاً باعث از میان رفتن سرقت اتومبیل‌ها از مراکز پرازدحام وسایط نقلیه شده است. سیستم «امنیت شاهدان» از یک کامپیوتر شخصی برای تحلیل و بررسی تصاویر ویدئویی مدار بسته استفاده می‌کند. نرم‌افزار تشخیص عکس می‌تواند بین حرکات انسان، حرکات حیوانات و اجسام جامد تفاوت قائل شود، هر چند که در تشخیص حرکات انسان در باران کمی مشکل دارد. اگر فعالیتی تردیدبرانگیز شناسایی شود، از طریق تلفن و تصاویری با کیفیت بالا به کارکنان شرکت BT فرستاده می‌شود. کل سیستم که در شرکت Neurody namics در کمبریج انگلستان ساخته شده، کمی بیش از ۲۵۰۰ پوند (۴۱۹۰ دلار) برای نصب، هزینه برمی‌دارد.(۹۵)

در فیرفاکس ویرجینیا، پلیس یک سیستم نظارت بر عکس‌ها را نصب کرده تا عکس افرادی که در تقاطع‌های ترافیکی از چراغ قرمز عبور می‌کنند را بردارد. اگر راننده‌ای توقف نکند، یک دوربین فعال شده و عکس او را برمی‌دارد. عکس همراه با جریمه ۵۰ دلاری نقض مقررات به آدرس خاطیان فرستاده می‌شود. از زمانی‌که این سیستم در ۲۵ ژوئیه تا آوریل و نوامبر سال ۱۹۹۷ نصب شد، بیش از ۴۵۹۸ مورد نقض مقررات در سه تقاطع ثبت شدند. این موارد منجر

---

1. Clive Norris
2. Gary Armstrong

به صدور ۱۸۷۳ برگ جریمه شد که از کل آن، ۶۸۲ قبض پرداخت گشت. منطقه الکساندریا[1] سیستم مشابهی را نصب کرد و در کشور تبدیل به شانزدهمین منطقه قضایی شد که از برنامه نظارت مبتنی بر عکاسی استفاده می‌کند. هدف اصلی این برنامه ایمنی است. اکثر حوادث ترافیک شهری که منجربه آسیب‌های جسمانی می‌شوند ناشی از افرادی هستند که از چراغ قرمز عبور می‌کنند. هدف دیگر این است که به مأموران پلیس این امکان داده شود تا به موضوعات دیگری هم رسیدگی کنند.[۹۶]

در ایران هم طی سال‌های اخیر، استفاده از دوربین‌های مداربسته و ویدئویی در معابر و خیابان‌های پرتردد متداول شده است و اکنون در بسیاری از شهرهای بزرگ و از جمله تهران، صدها دستگاه دوربین بر فراز ستون‌های فلزی نصب شده و وضعیت ترافیک و عبور و مرور خودروها را کنترل می‌نماید. از این دوربین‌ها برای پیگیری و ثبت تخلفات احتمالی نیز می‌توان استفاده کرد. تجربه نشان داده که نصب دوربین‌ها، حالت پیشگیرانه داشته و کمک بزرگی به مأموران انتظامی و راهنمایی و رانندگی کرده است.[۹۷]

در آریزونا، مقامات اقدام به نصب یک دوربین دوار به نام Sneaky Peak بر فراز ساختمان اصلی شهر کردند. سپس عکس‌های گرفته شده را به یک کامپیوتر ارسال می‌کنند و از آنجا در دسترس کاربران اینترنت که از وب استفاده می‌کنند، قرار می‌گیرد. بنا بر گفته دیوید کلی، مدیر این وب سایت؛ «این بزرگ‌ترین موفقیت در صفحه وب ما است». بعضی از دوربین‌ها به قدری کوچک هستند که می‌توان آنها را در کف دست پنهان کرد.[۹۸] شرکت Codex نوعی لنز ۳۲ × ۳۲ میلیمتری را از نوع زاویه عریض تبلیغ می‌کند که می‌تواند تصاویر ویدئویی فوری را به هر مانیتور یا دستگاه ضبط نوار ویدئویی بفرستد و در تاریکی نیز قابلیت رؤیت اجسام را دارد. گفته می‌شود میکروفون صوتی آن، صوت‌هایی از ۳۰ فوت دورتر را دریافت می‌کند.[۹۹] در ماه مه سال ۱۹۹۷ روزنامه نیویورک تایمز گزارش داد که شرکت توشیبا مشغول کار بر روی نوع جدیدی از تکنولوژی گرفتن عکس است که می‌تواند منجر به ساخت «دوربین کوچکی

---

1. Alexanderia

بر روی یک تراشه» شود. این نوع ریزدوربین‌ها را می‌توان در هر جا، حتی فریم عینک هم نصب کرد.(۱۰۰)

بنا بر اعلام مقاله‌ای در مارس سال ۱۹۹۸ در مجله تایمز، پلیس سوار در انگلستان در نظر دارد تا کلاه‌هایی با طراحی مخصوص که دارای دوربین جاسازی شده‌ای به اندازه دکمه پیراهن و میکروفون‌های ریز پرقدرت هستند، آزمایش کند. این تصاویر را می‌توان بر روی دستگاهی به اندازه واکمن ذخیره کرد و خود آنرا به کمربند افسر پلیس بست. همچنین می‌توان عکس‌ها را از روی یک لینک میکروویو به ایستگاهی در دو مایل دورتر ارسال کرد و به همکاران امکان داد تا بر اوضاع نظارت داشته و مشاوره‌هایی ارائه کنند. این دوربین‌ها که پشت کلاه نصب می‌شوند، عملاً برای طرف مقابل، غیرقابل رؤیت هستند.(۱۰۱)

۲۲ـ۱ـ ماهواره‌ها و تصویرپردازی

ماهواره‌ها می‌توانند با هزینه‌ای کمتر از هواپیما، عکس‌های در مساحت گسترده‌تری تهیه کنند. تصویرسازی ماهواره‌ای که زمانی محدود به دولت‌ها بود در اوایل دهه ۹۰ یعنی زمانی‌که آژانس فضایی روسیه به نام Sovinformsputnik فروش عکس‌هایی با کیفیت بالا را به‌صورت نقدی آغاز نمود، حالت تجاری پیدا کرد. در سال ۱۹۹۸ کنسرسیومی متشکل از شرکت فوق و شرکت‌های میکروسافت و Aerial Images و Digital Equipments و Kodak شروع به عرضه عکس‌هایی با تفکیک دو متر کردند که از ماهواره‌های تازه پرتاب شده روسی گرفته شده بودند. در آن سطح، می‌توان اتومبیل‌ها را از کامیون‌ها تشخیص داد، اما نمی‌توان شورلت را از یک فور تفکیک کرد. مشتریان علاقه‌مند به خرید این عکس‌ها، می‌توانند قبل از سفارش چاپ یا تکثیر بر روی سی‌دی، آنها را بر روی وب تماشا کنند. وب سایت موسوم به Terra Star هزار گیگابایت از داده‌ها را همراه تصاویر ماهواره‌ای گرفته شده از طرف مؤسسه «ارزیابی بوم‌شناختی» آمریکا و نیز عکس‌هایی از ماهواره‌های روسی ارائه می‌کند.(۱۰۲)

عکس‌های Sovinformsputnik از ماهواره‌های موقتی گرفته شده‌اند که با فیلم ظاهر شده

به زمین باز می‌گردند. در روش دیگری از ماهواره‌های دائم استفاده می‌شود تا عکس‌های خود را به‌صورت فوری به زمین بفرستند. شرکت Earth Watch از لانگ مونت کلرادو[1] در دسامبر سال ۱۹۹۷ از یک سایت روسی چنین ماهواره‌ای را پرتاب کرد. ماهواره موسوم به Eary Bird 1 عکس‌هایی با تفکیک ۳ متری ارسال می‌کند اما درست پس از ۴ روز شرکت Earth Watch تماس خود با این ماهواره را از دست داد و نتوانست دوباره ارتباطی برقرار کند. این شرکت در نظر داشت در سال ۱۹۹۸ ماهواره دیگری به نام Quick Bird با تفکیک کمتر از یک متر پرتاب کند. ماهوارهٔ دیگری با نام Ikonos با تفکیک یک متری برنامه‌ریزی شد که در سال ۱۹۹۸ زودتر از سایرین پرتاب شود. با تفکیک یک متری، می‌توان اشیائی به کوچکی جعبه تفنگ‌ها را تشخیص داد.[۱۰۳]

دولت آمریکا این حق را برای خود محفوظ داشت تا حسگرهای تجاری[2] را در زمان جنگ یا تنش بین‌المللی از کار بیندازد، همچنین فروش تصاویر ماهواره‌ای دارای لیسانس را به دولت‌های کوبا، لیبی، کره شمالی، ایران و عراق ممنوع اعلام کرد. اما در داخل دولت آمریکا درباره این موضوع که با وجود مخالفت وزارت بازرگانی آیا وزارتخانه‌های دفاع و خارجه می‌توانند اعمال نفوذ نمایند یا خیر، مناقشه‌ای برپا شد. وقتی کلینتون، رئیس‌جمهور وقت آمریکا در سال ۱۹۹۴ سیاست ملی کار با حسگرها از راه دور را تصویب کرد و راه برای مالکیت خصوصی ماهواره‌ای تصویرپرداز با تفکیک بالا را هموار ساخت، وزیر بازرگانی این اختیار را پیدا کرد تا بعد از مشورت با مقامات دفاعی و خارجه نسبت به مجوزهای اجرایی و مقررات مربوط به این نوع ماهواره‌ها اعمال نظر نماید. صنعت این نگرانی را دارد که سیاست خارجی ممکن است، تحریک شود تا بر فعالیت‌های تجاری، محدودیت‌های مخرب و ناموجهی را تحمیل نماید.[۱۰۴]

یکی از مسائلی که حساسیت خاصی دارد، بحث «کنترل شاتر»[3] است: یعنی محدود ساختن

1. Long mont Colorado
2. Commercaial Sensors
3. Shutter Control

گردآوری یا توزیع عکس‌های مربوط به مناطق جغرافیایی خاص. در ژوئیه سال ۱۹۹۸ وزارتخانه‌های بازرگانی و خارجه اعلام کردند که ماهواره‌های آمریکایی اجازه نخواهند داشت تا از اسرائیل عکس‌هایی با تفکیک و وضوح یک‌متری بگیرند، هر چند که عکس‌هایی با وضوح دومتری هنوز مجاز هستند. این تصمیم که سیاست درازمدت «آسمان آزاد»[1] دولت آمریکا را به پایان راه رساند به این علت اتخاذ شد که اسرائیل در هراس بود که عکس‌ها به‌دست دشمنانش بیفتند. رابرت موریس، یکی از تحلیلگران مؤسسه KPMG اظهار نگرانی کرد که دیگر کشورها نیز خواهان قرار مشابهی شده که در نتیجه باعث ایجاد مانع در بازار در حال رشد تصویرسازی تجاری خواهند شد.[۱۰۵]

مسئله دیگر این است که آیا داشتن حکم تفتیش برای مؤسسات مجری قانون که درصدد دسترسی به عکس‌های گرفته شده از شهروندان خصوصی و اموالشان هستند، ضروری خواهد بود یا خیر. در سال ۱۹۸۶ دیوان عالی آمریکا رأی داد که مؤسسه حفاظت از محیط‌زیست آمریکا می‌تواند از تأسیسات Dow Chemical در میدلند میشیگان عکس بگیرد، چرا که این عکس‌ها با استفاده از تجهیزات هواپیمایی نسبتاً متعارفی گرفته می‌شوند.[۱۰۶] در سال ۱۹۹۷ یکی از کشاورزان آریزونا به نام فلوید دان، در یک عکس ماهواره‌ای دیده می‌شود که مشغول پرورش پنبه است و ظاهراً مجوز آبیاری ندارد. اداره منابع آبی آریزونا، عکس را از ماهواره دولت فرانسه به نام SPOT به‌دست آورده بود. در کارولینای شمالی تصاویر ماهواره‌ای، فعالیت‌های ساختمانی گزارش نشده، توسعه کشاورزی و دیگر دستکاری‌های املاک و مستغلات را نشان می‌داد که می‌توانستند باعث مطرح شدن اظهارنامه‌هایی در خصوص مالیات بر اموال شوند.[۱۰۷]

عکس‌های ماهواره‌ای به‌شدت مورد استفاده مؤسسات نظامی و اطلاعاتی هستند. در آمریکا، مؤسسه ملی عکس‌برداری و نقشه‌کشی یک سیستم الکترونیکی ذخیره‌سازی و توزیع را طراحی کرده است که نقشه‌هایی مفصل و سه بعدی از ۸۰٪ سطح زمین برای تحلیلگران فراهم

1. Open Skies

خواهد ساخت.[۱۰۸] این سیستم، داده‌های اطلاعاتی الکترونیکی به‌دست آمده از انواع منابع، مانند مأموریت یکی از شاتل‌های فضایی (که قرار بود سال ۱۹۹۹ پرتاب شود)، ماهواره‌ها، هواپیماهای جاسوسی و موشک‌ها را با هم ترکیب می‌کند. این داده‌ها در یک بانک اطلاعاتی کنار هم قرار خواهند گرفت و در دسترس هر شخصی بر روی کره زمین خواهد بود. همچنین دسترسی به اطلاعات به‌صورت استاندارد درخواهد آمد تا مشکلاتی که در سیستم‌های اولیه وجود داشتند را (آنهایی که سیلی از انواع مختلف داده‌های اطلاعات الکترونیکی را بر سر تحلیلگران می‌باریدند)، برطرف کنند.[۱۰۹]

۲۳ـ۱ـ گیرنده‌های Van Eck

کامپیوترها، مانیتورها، چاپگرها، صفحه کلیدها، دستگاه‌های فاکس و دیگر تجهیزات الکترونیکی همگی از خود سیگنال‌های الکترومغناطیسی ساطع می‌کنند، در صورتی که خودشان در برابر شنود آسیب‌پذیرند. مانیتور قوی‌ترین سیگنال‌ها را تولید می‌کند و فرد استراق سمع کننده با کمک تجهیزات مناسب می‌تواند بر روی صفحه نمایش جداگانه‌ای اقدام به تماشای یک کپی از تصاویری نمایند که روی صفحه نمایش کامپیوتر مورد حمله به نمایش درآمده‌اند. در آوریل سال ۱۹۸۵ یک دانشمند هلندی به نام پروفسور «ویم وان اک»[1] جزوه‌ای را منتشر ساخت که در آن تخمین زده بود، حداکثر فاصله دریافت با استفاده از فقط یک گیرنده تلویزیونی معمولی حدود یک کیلومتر می‌باشد.[۱۱۰] در نتیجه انتشار مقاله او، سیگنال‌های ساطع شده از این دستگاه‌ها به نام «تشعشع وان اک»[2] معروف گشتند. این روش در نزد مؤسسات اطلاعاتی طبقه‌بندی شد، اما تا این کار انجام شود، زمان بسیاری از دست رفت. بنا بر گفته Winn Schwartaue مجله «کامپیوتر و امنیت» در شماره دسامبر سال ۱۹۸۵ خود به بحث درباره پدیده تشعشع وان اک پرداخت و در سال ۱۹۸۸ شرکت پخش برنامه‌های بریتانیا، بخشی از این پدیده را به روی آنتن‌های خود فرستاد. شوارتو می‌گوید، در سپتامبر سال

---

1. Wim Van Eck

2. Van Eck Radiation

۱۹۹۱ آنچه را به نمایش گذارد که عقیده داشت «اولین پخش ملی استراق سمع الکترومغناطیسی»[1] بر روی برنامه ژرالدو رویرا باشد. وی، همچنین گفت که جیم کارتر، رئیس بانک سکوریتی در هیوستون تگزاس نشان داد که چگونه می‌شود از دستگاه Diebold ATM اطلاعات مربوط به حساب را به‌دست آورد. سپس از این اطلاعات می‌توان برای تولید کارت‌های ATM جعلی نیز استفاده کرد. دستگاه‌های شنود وان اک را می‌توان به قیمت ۵۰۰ تا ۲۰۰۰ دلار از روی کاتالوگ‌های مختلف خریداری کرد.(۱۱۱)

در اواخر سال ۱۹۹۲ دان دلانی، یکی از کارآگاهان پلیس نیویورک گزارش داد که یک آنتن بر روی بالکن اتاقی در طبقه نوزدهم در ساختمان Helmsley واقع در نیویورک قرار داده شده و به طرف کمیکال بانک هدف‌گیری نمود. دفاتر وسط شهر این بانک، مأوای تعداد بسیاری از دستگاه‌های ATM و تأسیسات پردازش کارت‌های اعتباری این بانک بودند. شواهد عینی نشان می‌داد که بانک، هدف یکی از این حملات قرار گرفته، اما تا زمانی‌که پلیس، کار تحقیق و بازرسی را آغاز کند آنتن و اپراتور آن ناپدید شده بود.(۱۱۲)

۲۴ـ۱ـ حسگرهای متفرقه[2]

ارتش‌ها از رادار به شکلی گسترده برای شناسایی و تعیین محل تجهیزات دشمن و مؤسسات مجری قانون از آن برای مشخص کردن افرادی که در بزرگراه با سرعت غیرمجاز رانندگی می‌کنند، مورد استفاده قرار می‌گیرد. رادار عملاً به‌صورت یک چراغ جست‌وجوی الکترونیکی[3] کار می‌کند، یعنی امواج رادیویی ارسال کرده و بازتاب آنها را از روی اجسام موجود در منطقه بررسی می‌کند. با اندازه‌گیری مدت زمانی‌که طول می‌کشد تا یک سیگنال بازگردد، فاصله تا آن جسم تعیین می‌شود. مشاهدات تکراری این امکان را فراهم می‌سازد تا سرعت اجسام متحرک محاسبه شود. حسگرهای مبتنی بر رادار فعال می‌توانند از بین اکثر شاخ و برگ‌ها و خاک زمین

---

1. The First National Broad Cast of Elecrtomagnetic Eavesdropping
2. Mis Cell Aneous Sensors
3. Electronic Searchlight

عبور کند. دیگر حسگرها، رادار شخص دیگری را شناسایی کرده و از آن استفاده می‌کنند، یا در آن پارازیت می‌اندازند.[۱۱۳]

حسگرهای مادون قرمز تهیه عکس از اجسام گرم در مقایسه با زمینه سرد و برعکس را امکان‌پذیر می‌سازند. آنها می‌توانند با دریافت سیگنال‌های گرما، دید در شب را عملی نمایند. دید در شب با حسگرهایی که نور ستارگان یا مهتاب را چندصد برابر تقویت می‌کنند، نیز عملی می‌شود. حسگرهای ارتعاشی، مانند حسگرهای آکوستیک، لرزه‌ای یا فشار می‌توانند شلیک اسلحه را حس کرده و حرکت ماشین‌های بزرگ را شناسایی کنند. با حسگرهای مغناطیسی و گراویمتریک می‌توان وسایط نقلیه را از روی وزن یا عیار فولادشان تشخیص داد. حسگرهای شیمیایی می‌توانند حضور و جابجایی پستانداران بزرگ و برخی از فعالیت‌های صنعتی را تشخیص دهند. حسگرهای بیش از اندازه ریز را می‌توان با استفاده از تکنولوژی سیستم‌های میکروالکترود شیمیایی بر روی یک تراشه نیمه رسانا قرار داد. این نوع حسگرها می‌توانند هر چیزی را از شتاب و دما گرفته تا فشار و جریان سیالات شناسایی کنند.[۱۱۴]

در انگلستان یک سیستم خودکار تشخیص وسایط نقلیه می‌تواند پلاک خودروها را تشخیص داده و با استفاده از سیستم کامپیوتری اطلاعات جغرافیایی، رد وسایط نقلیه را بگیرد. این سیستم که هم در شب و هم در روز کار می‌کند، برای نظارت بر ترافیک و محافظت امنیتی مورد استفاده قرار می‌گیرد.[۱۱۵]

در ردوودسیتی کالیفرنیا پلیس با حسگرهای آکوستیک، آزمایش‌هایی انجام داده تا منبع شلیک گلوله را پیدا کند. میکروفون‌ها روی بام منازل و تیرک دیگر وسایل قرار می‌گیرند و از طریق خطوط تلفن به یک کامپیوتر مرکزی متصل می‌گردند. وقتی گلوله‌ای شلیک می‌شود، هر یک از میکروفون‌ها صدای آنرا در زمان‌های اندک متفاوتی دریافت می‌کنند. این تفاوت در زمان به کامپیوتر امکان می‌دهد تا از روش‌های مثلث‌بندی استفاده کند تا محل دقیق را شناسایی کرده و آنرا به‌صورت نقطه‌ای قرمز رنگ بر روی یک نقشه دیجیتالی نشان دهد.[۱۱۶]

از حسگرها در جنگ با موادمخدر نیز استفاده می‌شود. در سپتامبر سال ۱۹۹۷ رئیس

سیاست‌های موادمخدر دولت کلینتون به نام ژنرال بری مک کامزی، نقشه‌هایی را برای نصب سیستم‌های پیشرفته نظارت بر موادمخدر در طول مرز مکزیک ارائه داد. این سیستم شناسایی از اشعه ایکس، اشعه گاما و تکنولوژی گسیل پزیترون استفاده می‌کند که برای اولین‌بار برای شناسایی کلاهک‌های هسته‌ای در موشک‌های روسی ساخته شد. این سیستم که در ابتدا قرار بود در ۸ نقطه عبوری مرزی نصب شود، باعث کاهش جریان مواد غیرقانونی از مکزیک شد.[(۱۱۷)]

یکی از معضلات اساسی ایران در زمینه قاچاق موادمخدر وجود مرزهای طولانی در شرق کشور و همجواری با دو کشور افغانستان و پاکستان است. در کنار ده‌ها طرح بزرگ و کوچک مبارزه با قاچاقچیان، در سال‌های اخیر صحبت از بستن الکترونیکی مرزهای شرقی به میان آمده و حتی سازمان ملل متحد نیز اعلام کرده که حاضر است در پروژه مشترکی با همکاری ایران و پاکستان به اجرای طرح انسداد الکترونیکی مرزهای شرقی ایران، اقدام کند.[(۱۱۸)]

هر ساله حدود ۲۰۰ میلیارد ریال برای مبارزه با موادمخدر در مرزهای شرقی هزینه می‌شود، اما تا رسیدن به اجرای کامل چنین طرح‌های الکترونیکی که به تجهیزات فوق پیشرفته، نیروی انسانی، سرمایه‌گذاری سنگین و تکنولوژی ماهواره‌ای نیاز است، راهی طولانی در پیش‌رو می‌باشد. حسگرهای فعال و منفعل را می‌توان برای ردیابی محل افراد و اموال مورد استفاده قرار داد. تکنولوژی‌های فعال از منبع قدرت خود برای تولید و دریافت سیگنال‌ها از روی مانیتورها استفاده می‌کنند. می‌توان گیرنده ـ فرستنده‌های خودکار رادیویی کوچک را با گیرنده‌هایی در ده مایل دورتر دریافت کرد. والدین می‌توانند آنها را به لباس یا کوله‌پشتی فرزندانشان سنجاق کنند تا کودکان نوپای خود را پیدا کنند. سیستم‌های ایمنی اتومبیل مانند LoJack متعلق به شرکت Boston and Teletrack از کانزاس سیتی با اصول مشابهی کار می‌کنند و این امکان را فراهم می‌سازند تا وسایط نقلیه پیدا شوند. تکنولوژی‌های ردیابی انفعالی[1]، بدون برق و با پاسخ به میدان‌های الکترومغناطیسی[2] که از اسکنرها ساطع می‌شود، کار

---

1. Passive Tracking Technologies
2. Electromagnetic Fields

می‌کنند. می‌توان از یک کپسول شیشه‌ای به اندازه دانه برنج[1] و حاوی یک ریز تراشه[2] و یا آنتی[3] که به لباس سنجاق شده یا زیر پوست کار گذاشته شده، برای پیدا کردن بچه‌های گم شده یا ذخیره کردن اطلاعات دارویی استفاده کرد.[۱۱۹]

تکنولوژی مادون قرمز[4] در حال ترکیب شدن با یک پلاک هوشمند و نرم‌افزار ردیابی[5] است تا بر این امر نظارت داشته باشد که آیا وقتی کارگران به دستشویی می‌روند، دستان خود را می‌شویند یا خیر. این پلاک به طور ادواری صدای بیپ می‌دهد تا به کارمندان و کارگران یادآوری کند که دستان خود را بشویند یا حسگرهای موجود در اتاق که خود به یک کامپیوتر در دفتر مدیر متصل هستند، ارتباط برقرار می‌کند. در صورتی‌که کارگر مورد نظر از صابون استفاده نکند و به اندازه کافی جلوی دستشویی با آب جاری نایستد یک مورد نقض در کامپیوتر ضبط می‌شود. سیستم موسوم به «نگهبان بهداشت» که اولین سیستم در نوع خود است در کازینو توریپکانا در آتلانتیک سیتی نصب شده تا عادات ۲۰ نفر از سرآشپزها و ظرفشوها و مستخدمان را زیر نظر داشته باشد. در حالیکه طرفداران امیدوارند که این تکنولوژی، بحث بهداشت عمومی را برطرف کند (مطالعه‌ای نشان داده است که فقط $\frac{۲}{۳}$ مردم پس از رفتن به دستشویی دستان خود را می‌شویند). منتقدان، بحث حریم خصوصی را مطرح می‌سازند.[۱۲۰]

پرنده‌های بدون سرنشین[6] می‌توانند دوربین‌ها و دیگر حسگرها را در عملیات مورد استفاده قرار دهند. این نوع هواپیماهای کوچک با یک دوربین عدسی آئینه‌ای می‌توانند از یک کیلومتر دورتر تا، کمتر از یک سانتی‌متر تفکیک داشته باشند و با دوربین دوم می‌توانند درک عمق تا یک متری را عملی کنند. در ژانویه سال ۱۹۹۸ هفته‌نامه دفاعی جینز دیفنز گزارش داد که مؤسسه آمریکایی «پروژه‌های تحقیقاتی پیشرفته» برای توسعه وسایط هوایی ریز همراه با تکنولوژی‌های حسگر منحصر به‌فرد، ۱۲ میلیون دلار به‌صورت پاداش پرداخت کرده است. این

---

1. A rice-size Glass Capsule
2. Microchip
3. Antennae
4. Infrared Technology
5. Tracking Software
6. UAV

برنده‌ها بیش از ۱۶۰ میلی متر طول، ارتفاع، یا عرض (فاصله دو بال) نخواهند داشت و سیستم‌های ناوبری، ارتباطی و پردازشی را به‌صورت onboard با خود همراه خواهند داشت. پیشنهاد ۶ مقاطعه‌کار از طرف مؤسسه فوق برای تأمین سرمایه مورد موافقت قرار گرفت.(۱۲۱)

دیوید جن، استاد مهندسی برق در مدرسه فارغ‌التحصیلان نیروی دریایی و باب ویتالی، دانشجوی دوره دکترا، مشغول آزمایش با یک پرنده ریز دو اینچی با کنترل از راه دور هستند که می‌توانند به درون ساختمان‌ها پرواز کرده و محیط آنجا را ارزیابی نمایند. آنها در جست‌وجوی امکان تأمین برق این وسایل با یک منبع انرژی جداگانه هستند. یک آنتن هر یک از این پرنده‌ها را ردیابی کرده و یک پرتو میکروویو ارسال خواهد کرد تا انرژی آن تأمین شود.(۱۲۲)

در ژانویه سال ۱۹۹۷ محققان ژاپنی، آزمایش ریز پردازنده‌ها و ریزدوربین‌ها را که با جراحی در سوسک‌های آمریکایی جاسازی شده بودند، آغاز کردند. وزن این تجهیزات فقط ۱/۱۰ اُنس بود که حرکات سوسک را با سیگنال‌های راه دور تحت کنترل درآورده بودند. در ماه دسامبر، یک تیم تحقیقاتی در دانشگاه واندربیلت در تنسی، موفق به بستن قراردادی ۹۰۴ هزار دلاری با مؤسسه پروژه‌های تحقیقاتی پیشرفته دفاعی شد تا یک موجود روباتیک بسازد که بتوان از آن برای جاسوسی تصاویری در موارد گروگان‌گیری، کشف میدان مین و تحرکات نظامی استفاده کرد. هر کدّام از آنها ۲ اینچ طول داشتند و با فعال کننده‌هایی (شبیه آنهایی که یک پیجر را به ارتعاش درمی‌آورند) به جلو می‌خزیدند.(۱۲۳)

مارتین لیبکی[1] از افراد عالی‌رتبه در دانشگاه دفاع ملی آمریکا پیش‌بینی کرد که میدان نبرد آینده شاهد انواع مختلفی از حسگرها در سطوح گوناگونی از پوشش و تفکیک خواهد بود که به‌طور جمعی آنرا به گونه‌ای کامل نشان خواهند داد. وی حسگرها را به چهار گروه تقسیم کرد که عبارتند از: ۱ـ حسگرهای فراتر از موازنه‌ای[2] که عمدتاً در فضاپیماها کاربرد دارند، اما از

---

1. Martin Libicki
2. Far Stand-off Sensors

نوع حسگرهای زمین لرزه‌ای و آکوستیک نیز هستند، ۲ـ حسگرهای نیمه موازنه‌ای[1] از جمله پرنده‌های بدون سرنشین همراه با رادار چند طیفی، میکروویو، سینتتیک و توانمندی‌های اطلاعاتی الکترونیکی و نیز گویه‌های شناور فراساحلی با تجهیزات مشابه و رادار مبتنی بر سطح، ۳ـ حسگرهای in- place[2] از جمله انواع آکوستیک، گراویتریک، بیوشیمیایی و اپتیکی زمینی، ۴ـ حسگرهای تسلیحات[3] از جمله مادون قرمز، رادار انعکاسی و شناسایی نور.(۱۲۴)

۲۵ـ۱ـ جست‌وجو از بالای سر[4]

تمام حسگرها از نوع تکنولوژی سطح بالا نیستند که در این میان چشم و گوش انسان مثال خوبی محسوب می‌شود. سارقان، اطلاعاتی مانند شماره کارت اعتباری و PIN را با «جست‌وجو از بالای سر» انجام می‌دهند، یعنی تماشا از روی شانه‌های قربانیان و در مواقعی از فاصله‌ای معین با کمک یک تلسکوپ. در این شیوه آنها می‌توانند، شماره‌ای را همان‌طور که بر روی یک کارت تلفن یا دستگاه ATM پانچ شده، به‌دست آورند.(۱۲۵)

در یک مورد در انگلستان گزارش شد، دو نفر در صف دستگاه‌های ATM می‌ایستادند و شماره سریال مشتریان را می‌دیدند، رسیدهای دور ریخته شده را برمی‌داشتند، شماره حساب را روی کارت‌های ATM سفید کپی می‌کردند و سپس از این کارت‌ها برای بیرون کشیدن پول استفاده می‌نمودند. سارقان با استفاده از یک روش ساده‌تر از وجود خطایی در دستگاه‌های ATM انگلستان سود می‌بردند. این دستگاه‌ها ورود یک کارت تلفن را همان استفاده از کارت قبلی تصور می‌کردند و تنها کاری که لازم بود، دزدها انجام دهند به‌دست آوردن شماره سریال مشتریانی بود که در صف و جلوتر از آنها می‌ایستادند.(۱۲۶)

جای هیچ تعجبی نیست که سارقان، اقدام به خودکار کردن روش جست‌وجو از روی شانه خود کرده باشند. در یکی از حومه‌های شهر تورنتو به نام نیومارکت، یک گروه اقدام به نصب

---

1. Near Stand-off Sensors
2. In-Place Sensors
3. Weapons Sensors
4. Shoulder Surfing

دوربین مینیاتوری در یک ایستگاه پمپ بنزین کردند. وقتی مشتریان شماره سریال خود را برای استفاده از کارت تایپ می‌کردند، دوربین‌ها حرکات انگشتان آنان را روی نوار ویدئو ضبط می‌نمودند. متصدی پمپ بنزین که در این نقشه فعال بود، شماره حساب را از روی کارت‌خوان تهیه می‌کرد و بعد از قرار دادن شماره‌ها روی کارت‌های نانوشته، دزدان به سراغ دستگاه‌های ATM می‌رفتند تا به این حساب‌ها حمله ببرند و با ورود درست قبل از نیمه شب می‌توانستند دو برابر محدودیت روزانه پول بیرون بکشند. پلیس، افراد مظنون را دستگیر و رد صدها هزار دلار در حال خروج را پیدا کرد.(۱۲۷)

۲۶ـ۱ـ حریم خصوصی و پاسخگو بودن[1]

در اکثر کشورها اگر نگوییم، تمام آنها از جمله ایالات‌متحده در مکان‌های عمومی هیچ انتظاری از حفظ حریم خصوصی نمی‌رود. در هر صورت استفاده رو به رشد از دوربین‌ها و دیگر انواع حسگرها در این امکان برای گردآوری اطلاعات که ممکن است به دست پلیس محلی یا دیگر افراد برسد، مباحث مربوط به حریم خصوصی و پاسخگو بودن را مطرح کرده است. به‌عنوان مثال، متعاقب کشتار دانشجویان در سال ۱۹۸۹ در میدان تیان آن من[2] مقامات از عکس‌های گرفته شده از معترضان به‌وسیله دوربین‌های سیستم کنترل ترافیک استفاده کردند تا مخالفان حکومت را پیدا کنند. تصاویر به کرات در تلویزیون چین همراه با پیشنهاد جایزه، به نمایش درآمده و مقامات هم اقدام به بازجویی و شکنجه هزاران نفر کردند، به‌طوری که تقریباً تمام خاطیان شناسایی شدند.(۱۲۸)

در یکی از گزارش‌های پارلمان اروپا به نام «ارزیابی تکنولوژی‌ها در کنترل سیاست» آمده است که «پاسخگویی دموکراتیک تنها معیاری است که باعث تمایز سیستم مدرن کنترل ترافیک از تکنولوژی یافتن ناراضیان می‌شود». این گزارش که طیفی از روش‌های نظارت و سیستم UKUSA Echelon را مورد بررسی قرار داده بود، ۱۱ توصیه مطرح می‌کند که اولین توصیه

---

1. Privacy and Accontability

2. Tian an Men

چنین است که تکنولوژی‌ها، عملیات‌ها و رویه‌های نظارتی باید تابع آئین نامه‌هایی باشند که در معرض دید همگان قرار دارند تا پاسخگویی دموکراتیک همراه با مکانیسم‌هایی برای تضمین جبران خسارت در صورت بروز رویه‌ای غلط یا سوءاستفاده تضمین شود. برای تعیین اینکه چه کسی باید برای نظارت و مراقبت هدف قرار گیرد و چه‌اندازه از داده‌ها باید ذخیره، پردازش و مبادله شوند، ضروری است معیاری وجود داشته باشد که بر سر آن توافق شده است. دومین توصیه این است که تمام کدهای اجرایی باید تضمین کنند که تکنولوژی‌های جدید نظارت و مراقبت، در محدوده قوانین مناسب محافظت از داده‌ها قرار دارند.(۱۲۹)

دیوید برین، نویسنده داستان‌های علمی ـ تخیلی در اولین کتاب غیرداستانی خود به نام «جامعه شفاف» به بررسی جامعه‌ای می‌پردازد که حسگرها در اماکن عمومی و در تمام نقاط مستقر شده‌اند. اما ورودی این حسگرها فقط برای پلیس ارسال نمی‌گردد، بلکه در دسترس همگان قرار می‌گیرد. بنابراین تأثیر آن می‌تواند، افزایش پاسخگو بودن هرفردی باشد، از جمله نیروهای پلیس، درست همان‌طور که وقتی ایستگاه‌های تلویزیونی تصاویر ویدئویی را پخش می‌کردند، نشان می‌داد که پلیس، رادنی کینگ را کتک می‌زند.(۱۳۰)

۲۷ـ۱ـ خرابکاری[1]

این بخش به بررسی اقدامات خرابکارانه و تخریب اموال عمومی بر ضد سیستم‌های مخابراتی می‌پردازد از جمله عملیاتی که سرویس‌های تلفنی، جنگ الکترونیکی و حملات فیزیکی را دستکاری می‌کنند. در جنگ الکترونیکی از طیف الکترومغناطیسی استفاده می‌شود تا یک سیستم اطلاعاتی مورد نظر نابود شود. دو شکل از جنگ الکترونیکی مورد بررسی قرار گرفته است: پارازیت انداختن و استفاده از سلاح‌های دارای فرکانس رادیویی. در حملات فیزیکی از سلاح‌های متعارف‌تری استفاده می‌شود که ساختارهای مخابراتی را نابود کرده، یا به‌طور موقت خدمات آنرا تنزل داده و یا دچار وقفه می‌کنند. این حملات، یکپارچگی سیستم‌هایی را که به

---

1 Sabotage

خطر می‌اندازند، کاهش داده و در اغلب موارد در دسترس بودن آنها را برای مشتریان قانونی از میان برمی‌دارند.

۲۸ـ۱ـ دستکاری سرویس تلفن[1]

هکرها انواع راه‌ها را برای نشان دادن مهارت‌های خود در کامپیوترهای شرکت‌های تلفن پیدا کرده‌اند. مثلاً هکرهای موسوم به «استادان فریب» بعد از نفوذ به کامپیوترهای شرکت تلفن نیویورک، تلفنخانه یک رقیب را تبدیل به تلفن سکه‌ای کردند، به طوری‌که وقتی مورد استفاده قرار می‌گرفت، یک اپراتور وارد صحبت می‌شد و می‌گفت: «لطفاً یک سکه ۲۵ سنتی بیندازید».(۱۳۱)

یکی دیگر از ترفندهای محبوب در نزد هکرهای شرکت‌های تلفن این است که تماس اتوماتیک راه‌اندازی کنند تا تماس‌هایی را که به طرف هدف مورد نظر می‌باشند، مثلاً به طرف خطوط سکسی، انتقال دهند.(۱۳۲)

یکی از این خلافکارها، شماره اطلاعات عمومی اداره پلیس نیویورک را تغییر داد به طوری‌که تماس گیرنده‌ها پیامی را دریافت می‌کردند که با این جمله شروع می‌شد: «شما اداره پلیس نیویورک را گرفته‌اید. برای هرگونه واقعه اضطراری شماره ۱۱۹ را بگیرید. ما هم‌اکنون مشغول خوردن کمی پیراشکی همراه قهوه هستیم». صدای دیگری به گوش می‌رسید که داد می‌زد: «یک فنجان بزرگ قهوه!» صدای اول این طور صحبت را خاتمه می‌داد: «شما صحبت‌هایتان را کردید، ما خواهیم آمد. سرعت ما کمی کند است، با تشکر». این صدا به مدت ۱۲ ساعت تا نیمه شب پخش شد تا اینکه کارگری در شعبه ارتباطات، صبح روز بعد آنرا کشف کرد.(۱۳۳)

یک نوجوان سوئدی، کدهای یکی از شرکت‌های آمریکایی را شکست و با این کار توانست به صورت رایگان به تمام دوستان خود در آمریکا زنگ بزند.(۱۳۴)

1. Tampering With Phone Service

۲۹ـ۱ـ پارازیت انداختن[1]

پارازیت انداختن، شامل ارسال یک سیگنال برای تداخل[2] با سیگنال دیگر می‌باشد. از این روش بر ضد انواع مختلفی از فرکانس‌های سیگنال (به‌خصوص رادار و رادیو تلویزیون) استفاده شده است.

اشکال قدیمی رادار[3] به آسانی پارازیت پیدا می‌کردند، زیرا سیگنال را در یک فرکانس واحد، تولید می‌کردند. وقتی این فرکانس شناخته می‌شد، سیگنال بازگشتی به آسانی پارازیت می‌شد، اما رادارهای مدرن از یک فرکانس به فرکانس دیگر می‌پرند. بنابراین امروزه، افرادی که پارازیت ایجاد می‌کنند باید بتوانند سیگنال را رهگیری کنند، فرکانس آنرا تعیین نمایند، مطابق با آن سیگنال، ایجاد پارازیت را تنظیم کنند و به سرعت یک blur back ارسال کنند تا طول و مقاومت سیگنال منعکس شده را به حداقل برسانند. مارتین لیبکی، می‌گوید که رادار هنوز آسان‌تر از سیستم‌های ارتباطی مدرن (که از جهش فرکانس، طیف گسترده و تکنولوژی multiplexing تقسیم کد استفاده می‌کنند و به این ترتیب رهگیری و پارازیت انداختن را مشکل می‌سازند) پارازیت‌دار می‌شود. با تکنولوژی‌های فشرده‌سازی دیجیتالی و redundancy سیگنال می‌توان ارتباطات را از سر گرفت، حتی اگر بخش عمده‌ای از آن پارازیت‌دار شده باشد.(۱۳۵)

ارتباطات میکروویو را می‌توان پارازیت‌دار کرد. در سپتامبر سال ۱۹۹۷ یک شرکت روسی به نام Avaconversia اعلام کرد که یک پارازیت‌انداز ۴ واتی با قیمتی کمتر از ۴ هزار دلار می‌تواند سیگنال‌های میکروویو را از «سیستم تعیین موقعیت جهانی» (GPS) در یک شعاع ۲۰۰ کیلومتری پارازیت‌دار کند. سیستم تعیین موقعیت جهانی که ابتدا در وزارت دفاع آمریکا و برای کاربردهای نظامی طراحی و ساخته شد، متشکل از ۲۴ ماهواره است که به‌طرز فزاینده‌ای در سرتاسر جهان برای ناوبری و دیگر کاربردها مورد استفاده قرار می‌گیرد.

---

1. Jamming
2. To Interfere
3. Traditional Forms of Radar

پارازیت‌اندازهای ساخت روسیه نیز به تروریست‌ها و دیگر دشمنان، ابزاری می‌دهند تا سیستم‌های ناوبری هواپیما، موشک‌های هدایت شونده با GPS و دیگر سیستم‌ها را که متکی به سیستم تعیین موقعیت جهانی هستند، دچار اختلال نمایند. اما اینکه این نوع پارازیت انداختن می‌تواند عملاً باعث سقوط هواپیما شود یا خیر، هنوز ناشناخته است.[۱۳۶]

۳۰ـ۱ـ سلاح‌هایی با فرکانس رادیویی[۱]

سلاح‌هایی با فرکانس رادیویی (RF) دستگاه‌هایی هستند که اقدام به گسیل تشعشعات الکترومغناطیسی در طیف رادیویی می‌کنند. تأثیر این عمل، از کارانداختن یا نابودسازی تجهیزات الکترونیکی است که این تشعشعات به آنها می‌رسند. هدف ممکن است یک کامپیوتر، گیرنده‌های مخابراتی، سیستم ناوبری و یا سیستم هشدار باشد. این سلاح‌ها می‌توانند پهن باند یا باریک باند، جهتی (directional) یا غیرجهتی، تک پالس، پالس مکرر یا موج دائم باشند. دستگاه‌هایی که پالس‌های پهن باند، گسیل می‌کنند به نام سلاح‌هایی با پالس الکترومغناطیسی (EMP) معروف هستند. کارلو کاپ، از تحلیلگران مستقل مسائل دفاعی و مهندس استرالیایی که قسمت اعظم مطالب این بخش را فراهم کرده، پیامدهای ناشی از سلاح‌های فرکانس رادیویی و پالس الکترومغناطیسی را به‌طرز گسترده‌ای مورد مطالعه قرار داده است.[۱۳۷]

دستگاه‌های پهن باند[۲] یک transient الکترومغناطیسی تیز و پالس‌دار تولید می‌کنند که می‌تواند جهتی یا غیرجهتی باشد و همچنین می‌توان آنرا یک‌بار و یا به‌طور مکرر گسیل کرد. میدان transient معمولاً یک پالس کوتاه مدت‌دار (spike) با ولتاژ قوی یا ringing روی کابل‌ها و سیم‌کشی لخت ایجاد می‌کند. این امر می‌تواند مدارهای نیمه‌رسانای لخت را دچار آسیب یا وقفه نماید. دستگاه‌هایی که در این گروه قرار دارند، شامل پالس الکترومغناطیسی هسته‌ای، EMP مولد جریان و دستگاه‌های پلاتین مولد جرقه یا spark-gap هستند. از بین

1. Radio Frequency Weapons
2. Broadband devices

اینها، دستگاه‌های پالس الکترومغناطیسی هسته‌ای، قدرتمندترین و مخرب‌ترین دستگاه‌ها محسوب می‌شوند. آنها می‌توانند هم خسارت حرارتی و هم از کار افتادگی الکتریکی ایجاد کنند. در فوریه سال ۱۹۹۸ دیوید شراینر، یکی از مهندسان ارشد مؤسسه جنگ‌های الکترونیکی که از تأسیسات بخش سلاح‌های نیروی دریایی در china lack بازنشسته شده است، در مقابل کمیته مشترک اقتصادی در کنگره آمریکا گواهی داد که وی با موفقیت در حیاط‌خلوت خانه خود یک اسلحه فرکانس رادیویی پهن باند با سوئیچ‌های پلاتین مولد جرقه روغنی از روی مصالحی که با پست سفارش داده شده بودند، با هزینه‌ای معادل ۵۰۰ دلار ساخته است. این دستگاه که آنرا دستگاه الکترومغناطیسی transient می‌نامید، دو هفته پس از اینکه کارش را شروع کرد، آماده آزمایش شده بود. این دستگاه از دو سیم‌پیچ احتراق و یک باتری برای تأمین برق، یک پمپ سوخت اتومبیل و فیلتر برای گردش روغن و از روغنی که به‌طور متداول در دسترس است، استفاده می‌کند. این دستگاه از باند فرکانس رادیویی یا باندهای میکروویو پایین‌تر، امواجی را تولید می‌کند. شراینر تخمین زده است که این دستگاه برای تروریست‌ها سلاح‌های جالب توجهی خواهد بود که می‌توان آنها را در وانتی کوچک گذاشت و در یک پارکینگ مورد استفاده قرار داد، یا در هنگامی‌که وانت عبور می‌کند به طرف ساختمان‌ها هدف گرفت.[۱۳۸] اطلاعات فنی برای ساخت آنها از منابع آزاد در دسترس هستند. در اکثر موارد، این دستگاه‌ها باعث بروز وقفه در سیستم طرف قربانی می‌شوند، نه اینکه خسارت دائم ایجاد کنند.[۱۳۹]

سلاح‌های فرکانس رادیویی باریک باند[1] در محدوده باند فرکانس نسبتاً باریک، یک موج حامل فرکانس رادیویی (مداوم یا پالس‌دار) ایجاد می‌کنند. موج حامل می‌تواند VHF (فرکانس بسیار بالا)، UHF (فرکانس بیش از حد بالا)، یا در باند میکروویو باشد. این موج با سیم‌کشی برق جفت می‌شود یا در مورد دستگاه‌های میکروویو، مستقیماً از طریق روزنه‌ها و شکاف‌های موجود به شاسی دستگاه‌ها متصل شده و موج‌های عمودی یا standing با ولتاژ زیاد تولید

1. Narrow Band RF Weapons

می‌کند. این نوع موج‌ها می‌توانند اجزای نیمه‌رسانا را تخریب کنند یا در کار آنها وقفه ایجاد نمایند. سلاح‌های فرکانس رادیویی باریک باند، معمولاً از نظر تأثیری که دارند، از نوع جهتی محسوب می‌شوند.(۱۴۰)

قدرتمندترین سلاح‌ها در این گروه، دستگاه‌های میکروویو پرقدرت هستند. آنها معمولاً تشعشع خود را با فرکانس‌هایی بین ۱ تا ۳۵ گیگاهرتز گسیل می‌کنند و به این ترتیب چند گیگاوات یا ده‌ها گیگاوات توان تولید می‌کنند، همچنین می‌توانند در مسافت‌های صدها متر یا بیشتر میدان فرکانس رادیویی با توان ده‌ها کیلووات در هر متر را ایجاد کنند. عملیات می‌تواند تک پالسی، پالس مکرر یا موج مداوم باشد. این نوع سلاح‌ها می‌توانند در مقایسه با روش‌های جهتی جنگ الکترونیکی، خسارات بیشتر و قابل ملاحظه‌ای را به‌وجود آورند، زیرا اهداف را در معرض صد تا هزار بار توان بیشتر قرار می‌دهند.

«وین شوارتاو» سلاح‌های قابل حمل با فرکانس رادیویی را «تفنگ‌های فرکانس رادیویی پرانرژی»[1] می‌نامد. خروجی توان آنها بین چند کیلووات تا صدها کیلووات است. با وجودی‌که تأثیر آنها به مراتب کم قدرت‌تر از تأثیر سلاح‌های میکروویو پرقدرت است، اندازه کوچک و منبع برق جمع و جور آنها باعث می‌شود که این سلاح‌ها وسیله جالب توجهی برای تروریست‌ها یا گروه‌های عملیات ویژه شوند تا در عوض نابودی تجهیزات، در کار آنها وقفه ایجاد کنند.

قطعاتی که در برابر سلاح‌های فرکانس رادیویی بسیار آسیب‌پذیرند نیمه‌رساناهای MOS و نیمه‌رساناهای پرسرعت دو قطبی (bipolar) هستند. دستگاه‌ها متعاقب از کار افتادن ابتدایی برقشان، از طریق تأثیر ناگهانی و به‌شدت که با ادامه پمپاژ انرژی به درون دستگاه از طرف منبع تغذیه خود ایجاد می‌گردد، دچار آسیب حرارتی می‌شوند حتی اگر استقامت میدان برای بروز وقفه کامل ناکافی باشد، ممکن است خسارت روی دستگاه هدف گرفته شده به قدری باشد که دیگر آن دستگاه قابل اتکا نبوده و یا به‌طور موقت از کار بیفتد. ممکن است کامپیوترها از

1. High – energy radio Fre/ quency guns

فعالیت بازمانند و با تأثیر آبشار مانند احتمالی روی دیگر تجهیزات یا سیستم‌های بزرگ‌تـر کـه کامپیوترها در آنها مستقر می‌شوند، همراه باشند.

استفاده موفقیت‌آمیز از سلاح‌های فرکانس رادیویی مستلزم شناخت اثرات هدف آنها است. ارزیابی تأثیر آنها می‌تواند مشکل باشد، چراکه ممکن است ایـن تـأثیرات بلافاصـله بـه چـشم نیایند، به‌خصوص در سلاح‌هایی که از قدرت کمتری برخوردارند.

گزارش‌های انگشت‌شماری از استفاده سلاح‌های فرکانس رادیـویی بـه‌دسـت جنایتکـاران، ارائه شده است.

تفنگ‌های الکترونیکی[1] وجود دارند که می‌توانند رادیوهای پرتابل[2] و تلفن‌های همراه[3] را از کار بیندازند. یکی از ژنرال‌های روسی نسبت به تعداد فزاینده مواردی که طی آن، تروریست‌هـا از دستگاه‌های الکترومغناطیسی استفاده کرده‌اند، اظهار نگرانی کرده و گفته اسـت، خلافکارهـا در کشورهای غربی از جمله سوئد از سلاح‌های فرکانس رادیویی برای حمله بـه سیـستم‌هـای هشدار مؤسسات مالی استفاده کرده‌اند. وی هشدار می‌داد که تروریست‌هـا بـا اسـتفاده از ایـن سلاح‌ها می‌توانند هرج و مرج عظیمی را ایجاد کنند. آنها می‌توانند سلاح‌های خود را به طـرف مراکز کامپیوتری نشانه روند و کارهایی که متکی به کامپیوتر است را به هـم بریزنـد، همچنـین می‌توانند سلاح‌های میکروویو را به طرف ترافیک موجود بر روی بزرگراه‌هـا هـدف بگیرنـد و باعث بد کار کردن اتومبیل‌ها و بروز سانحه گردند. آزمایش‌هـای ارتـش سـوئد نـشان داد کـه سلاح‌های پالس الکترومغناطیسی که با استفاده از مصالحی که بـه‌آسـانی در دسـترس هـستند، ساخته می‌شوند، قادرند از فاصله ۳۰ متری باعث خرابی دائم اتومبیل‌ها و از فاصـله ۹۰ متـری باعث از کار افتادن موتور آنها گردند.(۱۴۱)

مجله Techwire مقاله دیگری منتشر کرد و حداقل برخی از ادعاها را در مـورد اسـتفاده از سلاح‌های فرکانس رادیویی از اعتبار انداخت. این مقاله گزارش می‌داد که مایکـل کـر کـوران،

---

1. Electronic Guns
2. Portable Radios
3. Mobile Phones

تحلیلگر اصلی در گروه جنگ‌های اطلاعاتی «مؤسسه تحقیق و ارزیابی دفاعی» انگلستان می‌گوید که اظهارنظرهایی درباره خلافکاران فضای سایبر و تروریست‌هایی که از سلاح‌های فرکانس رادیویی برای استخراج پول از بانک‌ها استفاده می‌کنند، شده اما یاوه‌ای بیش نبوده است. وی می‌گفت: «هیچ سلاح فرکانس رادیویی وجود ندارد که هر کس در هر موقعیتی که قرار دارد بر ضد بانک‌ها مورد استفاده قرار دهد. آنها در آینده به وجود خواهند آمد، اما مسلماً هنوز عملی نشده‌اند. گزارش‌های منتشر شده در برخی از روزنامه‌ها در طول سال‌های گذشته خیال‌پردازی محض بوده است».[۱۴۲]

من نتوانستم هیچ یک از گزارش‌های مربوط به جنایتکاران یا تروریست‌ها را که از سلاح‌های فرکانس رادیویی برای هدف خاصی استفاده می‌کنند، تأیید نمایم. جورج اسمیت در مقاله‌ای به نام «سلاح پالس الکترومغناطیسی: chapacapraهای جنگ اطلاعاتی» شایعاتی که درباره استفاده آنها نزد هکرها و تبهکاران روسی وجود دارد را زیر سؤال برده است. تنها نقطه جالب توجه این است که هیچ‌کس عملاً یک دستگاه پالس الکترومغناطیسی برای بررسی عمومی باز تولید نکرده است.[۱۴۳]

یک کمیسیون تخصصی در زمینه حفاظت از زیرساخت‌های حیاتی، اقدام به بررسی تهدید سلاح‌های پالس الکترومغناطیسی کرده است. آنها به این نتیجه رسیدند که سلاح‌هایی با ماهیت این‌چنینی هنوز در مراحل آزمایشگاهی هستند.[۱۴۴]

کاپ[1] می‌گوید که وی چیزی از موارد شناخته شده درباره تجهیزات نهایی شده فرکانس رادیویی پرانرژی نشنیده است، اما انتظار دارد که وقتی نیروهای پلیس اقدام به استفاده گسترده از دستگاه‌های transient الکترومغناطیسی یا فرکانس رادیویی پرانرژی می‌نمایند (که برای متوقف کردن اتومبیل‌ها از طریق، از کار انداختن سیستم احتراق و تزریق سوخت آنها طراحی شده‌اند) مشکلات تکثیر خود را نشان دهند.

---

1. Kopp

۳۱ـ۱ـ کاربرد جنگ الکترونیک در جنگ خلیج‌فارس

آمریکایی‌ها یک‌بار دیگر هم از تکنیک جنگ الکترونیک برای منهدم ساختن تأسیسات ارتباطی عراق در جنگ اول خلیج‌فارس در سال ۱۹۹۱ استفاده کرده بودند. در جنگ سال ۲۰۰۳ موضوع مهم، نابود یا بی‌خاصیت کردن سیستم‌های اطلاعاتی کلیدی عراق با روش‌های الکترونیک یا فیزیکی بود. در ساعات اولیه آغاز عملیات توفان صحرا، سلاح‌های ضدتشعشع که از هلی‌کوپترها و هواپیماها شلیک می‌شدند، شبکه دفاع هوایی عراق را فلج کردند. نوارهایی از.فیبر کردن که از موشک‌های تام هاوک بر فراز سیستم سوئیچینگ شبکه برق عراق تخلیه شد، باعث اتصال برق و خاموشی‌های گسترده در شبکه برق عراق گشت. یک بمب هدایت شونده که توسط بمب‌افکن آمریکایی رها شد از هواکش سیستم تهویه مطبوع مرکز تلفن عراق در بغداد وارد ساختمان شد و تمام شبکه زیرزمینی کابل کواکسیال که فرماندهی عراق را به واحدهای زیردستش مرتبط می‌ساخت، از بین برد. پس از اینکه مراکز فرماندهی و کنترل از کار افتادند، نیروهای مهاجم درصدد نابودی سیستم‌های رادار عراق برآمدند در حالیکه رادارها نمی‌توانستند فضای نبرد را ببینند، بنابراین عراق شانس کمی برای پیروزی داشت. ویروس‌های کامپیوتری نیز از جمله عوامل اختلاف در سیستم ارتباطی عراق بودند. براساس یک گزارش، ویروسی که در یکی از ICهای چاپگر جاسازی شده بود، چاپگرها و مانیتورهای تحت سیستمّ عامل ویندوز[1] را از کار انداخت. این چاپگر از فرانسه خریداری شده و در مقر دفاع هوایی عراق نصب گشته بود. گفته می‌شد که ویروس مذکور توسط آژانس امنیت ملی آمریکا و CIA طراحی شده که به نام ویروس 91/AF بود.

همزمان با آغاز حمله آمریکا به عراق، پخش برنامه‌های رادیوی عراق متوقف شد و به جای آن برنامه‌های رادیو آمریکا به زبان عربی پخش می‌شد. به گزارش ایسنا و به نقل ازخبرگزاری فرانسه، در برنامه عربی رادیو آمریکا ادعا شد که «آزادی آغاز شده است».

تازه‌ترین نمونه اختلال در شبکه‌های تلویزیونی در زمان جنگ اخیر آمریکا ـ عراق رخ داد.

---

1. Windows

در شب آغاز جنگ عراق، تلویزیون دولتی عراق به‌طور موقت دچار اختلال شد. به طوری‌که برنامه‌های معمول خبری و سرودهای میهن‌پرستانه با خطوط افقی رنگی که از یک منبع ناشناخته می‌آمد، جایگزین شده بود. پس از آن، این شبکه بارها شاهد تلاش‌هایی برای ایجاد اختلال به روش‌های نظامی و متعارف‌تر بود.[(۱۴۵)]

تدوین راهبرد امنیت الکترونیک در کشور و ایجاد سازمانی در عالی‌ترین سطح اجرایی برای تدوین سیاست‌های اجرایی ناشی از راهبردهای مصوب امنیت الکترونیک و نظارت بر پیاده‌سازی آنها ضروری است.

جنگ الکترونیک از موارد بسیار حائز اهمیت است. در جنگ خلیج‌فارس در سال ۱۹۹۱ موضوع پراهمیت، از بین بردن یا بی‌خاصیت کردن سیستم‌های اطلاعاتی کلیدی عراق با روش‌های الکترونیک یا فیزیکی بود. در ساعات اولیه آغاز عملیات توفان صحرا، سلاح‌های ضدتشعشع که از هلی‌کوپترها و هواپیماها شلیک می‌شدند شبکه دفاع هوایی عراق را فلج کردند. نوارهایی از فیبر کربنی از موشک‌های تام‌هاک بر فراز سیستم سوئیچینگ شبکه عراق تخلیه شد و باعث اتصال برق و خاموشی‌های گسترده در شبکه عراق گشت.

در رابطه با نابودی مراکز مخابراتی در عراق باید گفت، یک بمب هدایت شونده[1] که توسط یک بمب‌افکن رها شد از هواکش سیستم تهویه مطبوع مرکز تلفن عراق در بغداد وارد ساختمان شد و تمام شبکه زیرزمینی کابل کواکسیال که فرماندهی عراق را به واحدهای زیردستش مرتبط می‌کرد، از بین برد. پس از اینکه مراکز فرماندهی و کنترل از کار افتادند نیروهای مهاجم درصدد نابودی سیستم‌های رادار عراق برآمدند در حالی که رادارها نمی‌توانستند فضای نبرد را ببینند، بنابراین عراق شانس کمی برای پیروزی داشت.

ویروس کامپیوتری نیز از مواردی است که موجب اختلالاتی در عراق شد، به طوری که ویروسی که در یکی از ICهای یک چاپگر جاسازی شده بود، چاپگرها و مونیتورهای تحت سیستم عامل ویندوز را از کار انداخت. این چاپگر از فرانسه خریداری شده بود و در مقر دفاع

1. Guided Bomb

هوایی عراق نصب گردید. گفته می‌شود که ویروس توسط آژانس امنیت ملی آمریکا و سیا طراحی شده بود، نام ویروس 91/AF می‌باشد.

از وسایل ارتباط جمعی، تلویزیون و ماهواره‌های توزیع خبر، استفاده‌های گوناگونی برای تبلیغات و تشویق سربازان به تسلیم، می‌شد. در این موارد صدام اشتباهات دیگری هم مرتکب شد، از جمله اینکه سربازان و ارتش عراق آماده فداکاری و از خودگذشتگی هستند، اما آمریکا تحمل تلفات را ندارد. بنابراین سازمان و افسران عراقی متوجه شدند که آنها هستند که باید کشته شوند، لذا زودتر تسلیم شدند. در آمریکا از تهاجم سربازان عراقی به نوزادان در کویت نشان داده شد. در این فیلم، سربازان، نوزادان را از دستگاهی که مخصوص نگهداری آن به‌دلیل زایمان زودرس بود، خارج می‌کردند. این فیلم را در خلال ۴۴ روز جنگ، ۸ بار رئیس‌جمهور آمریکا مشاهده کرده بود و همچنین در جلسه رأی‌گیری سنای آمریکا در مورد دخالت در عراق نیز چندین بار پخش شده بود. دخالت آمریکا در این جنگ فقط با ۵ رأی موافق بیش از آرا مخالف تصویب شد. بعدها شبکه CBS به‌دنبال منبع این فیلم بود و متوجه شد که تنها شاهد عینی ماجرا، دختر ۱۵ ساله سفیر سابق کویت در آمریکا بوده است.

جنگ‌های اطلاعاتی از نوع غیرفیزیکی و غیرروان‌شناختی مدنظر می‌باشند، مثلاً انهدام مرکز مخابراتی با پرتاب بمب یا مواد انفجاری مورد نظر نیست. پیشرفت‌های رایانه‌ای با پیشرفت‌های بسیار خوبی در ساخت سنسورها همراه گشته است. اکنون سنسورهای بسیار ارزان، کوچک و دقیقی ساخته می‌شوند که به آسانی با سایر فناوری‌ها ارتباط برقرار می‌کنند. به‌دلیل رشد سیستم‌های اتوماتیک و افزایش قابلیت ارتباط، زیرساخت‌های مهم کشور به شکل روزافزونی به یکدیگر وابسته می‌شوند، سیستم‌های توزیع برق انرژی یا خدمات اضطراری، حمل‌ونقل با رایانه‌ها و مخابرات راه دور پشتیبانی می‌شوند. اگر تمام شبکه مخابراتی کشور برای مدت یک هفته از کار بیفتد، چه عواقبی برای شهروندان ایجاد می‌شود. برپایی یک ارتش سنتی کم‌هزینه نیست. یک جنگنده بیش از صد میلیون دلار قیمت دارد، علاوه بر آن باید هزینه ناوها، تانک‌ها، ماهواره‌های جاسوسی و افراد مسلح را نیز در نظر گرفت. در مقایسه، مبلغی

بین ۱ تا ۱۰ میلیون دلار برای تأمین هزینه تیمی متشکل از ۱۰ تا ۲۰ هکر برای جنگ اطلاعات کافی است. این تیم با همین مبلغ را می‌توان به آخرین مدل‌های رایانه‌ای نیز مجهز ساخت. ابزارهای Haching را نیز می‌توان بدون هزینه در سرتاسر سایت‌های اینترنتی جهان به‌دست آورد.

حفاظت از زیرساختار ملی حیاتی، شامل بخش‌های مخابراتی، بانکی و مالی، تولیدی و توزیع برق، ذخیره و توزیع نفت و گاز، منابع آب، حمل‌ونقل، خدمات اضطراری و خدمات دولتی است.-باید اقدامات گوناگونی در مورد حفاظت از زیرساختار ملی حیاتی به‌عمل آورد. برای نمونه، می‌توان از ایجاد مرکز هماهنگی پاسخ اضطراری به حملات رایانه‌ای نام برد. چنین مرکزی پس از واقعه از کار افتادن شبکه اینترنت در سال ۱۹۸۸ در آمریکا اتفاق افتاد. این مرکز به طور ۲۴ ساعته فعال بوده و با فروشندگان سیستم‌های کامپیوتری در مورد کنترل حوادث رایانه‌ای همکاری می‌کرد. البته مراکز پاسخ اضطراری در آمریکا محدود به این جا نبوده و مراکز متعدد دیگری نیز تأسیس شده‌اند.

زیرساختار ملی حیاتی در حقیقت کلیه سرویس‌هایی است که از حیات و زندگی افراد در کشور پشتیبانی می‌کند. این زیرساختار در معرض خطرات و تهدیدات متعددی قرار دارد و با توسعه اجتناب‌ناپذیر استفاده از تکنولوژی‌های رایانه‌ای و شبکه‌ای، ارتباطات درونی این ساختار بیشتر و بیشتر شده و خطرات و آسیب‌پذیری‌های جدیدی به‌وجود می‌آید. تدوین راهبرد امنیت الکترونیک در کشور، ایجاد سازمانی در عالی‌ترین سطح اجرایی برای تدوین سیاست‌های اجرایی ناشی از راهبردهای مصوب امنیت الکترونیک و نظارت بر پیاده‌سازی آنها، بازرسی و کنترل سیستم زیرساختار حیاتی کشور، تدوین استانداردهای لازم، سرمایه‌گذاری در چارچوب راهبردهای مصوب و سیاست‌های اجرایی ناشی از آنها در امر تحقیقات، آموزش و فرهنگ‌سازی، ایجاد تشکیلات پاسخ سریع به وقایع مربوط به جنگ اطلاعات، پیشنهاد لوایح قضایی برای تطبیق با الزامات ناشی از فناوری اطلاعات، الزام به تأمین امنیت اطلاعات در سرمایه‌گذاری مربوط و ایجاد فناوری ملی ـ بومی در امنیت الکترونیک ضروری است.[۱۴۶]

فصل دوم

۱ـ۲ـ حملات فیزیکی[1]

چندین حادثه گزارش شده از خرابکاری فیزیکی بر ضد سیستم‌های مخابراتی وجود داشته است. در یک مورد، خرابکارها در پورتوریکو اقدام به قطع یک خط فیبرنوری کردند که برای دفتر دولت، یک هتل برجسته و دیگر تأسیسات عمومی بود تا با این عمل اعتراض خود را نسبت به فروش برنامه‌ریزی شده شرکت تلفن پورتوریکو نشان دهند. فدریکو تورزمونتالوو[2]، رهبر اتحادیه بخش عمومی می‌گفت: «آنها امید داشته‌اند تا با نشان دادن عمق خصومت کارگران، خریداران بالقوه را وحشت‌زده نمایند. خسارت‌های برآورد شده از جمله در پاییز ۱۹۹۷ بالغ بر ۲۰۰ هزار دلار بود».[۱۴۷]

در ژانویه سال ۱۹۹۷ در سیستم تلفن الجزایر، خرابکاری ایجاد شد. بنا بر گزارش‌های منتشر شده، حملات مکرر خرابکارها باعث بروز وقفه در خدمات منطقهٔ حسین دی الجزایر شده بود. اقدامات خرابکارانه مشابهی نیز باعث بروز کمبود پراکنده گاز و برق در پایتخت شده بود. دولت، شبه‌نظامیان مسلمان را بابت این خرابکاری‌ها مقصر می‌دانست و می‌گفت: این کارها بیش از ۲ میلیارد دلار خسارت به اقتصاد کشور وارد کرده است.[۱۴۸]

در یک دوره سه روزه در نوامبر سال ۱۹۹۷ خرابکارها در منطقه بوستون، باعث بروز وقفه

---

1. Physical Attacks
2. Federico Tourez Montaloo

در خدمات تلویزیون کابلی Media One برای حدود ۴۰ هزار مشترک شدند. آنها همچنین در خدمات ارائه شده راه دور از طرف شرکت مخابراتی Teleport برای حدود ۳۵۰ شرکت وقفه ایجاد کردند. خرابکارها ظاهراً از ۸۰ تیر برق بالا رفته بودند و کابل‌های فیبر نوری به ضخامت یک اینچ را در مجراهایی که مورد اشتراک دو شرکت بود، قطع می‌کردند. به محض اینکه خرابی‌ها گزارش می‌شد، سرویس‌ها به سرعت از سر گرفته می‌شدند. مشتریان Media One بابت خدمات از دست رفته، یک اعتبار یک روزه دریافت کردند.[۱۴۹]

در سال ۱۹۸۵ یک گروه تروریستی به نام Middle Core Faction به سیستم ریلی مسافران برون شهری ژاپن حمله کردند و باعث به‌وجود آمدن وقفه‌ای سراسری در اوج ساعت ترافیک شدند. این گروه به کابل‌های ارتباطی و برق استراتژیک که به کنترل‌های کامپیوتری سیستم ریل آهن متصل می‌شدند، به‌شدت آسیب رساندند و در فرکانس‌های رادیویی پلیس و امداد پارازیت می‌انداختند تا واکنش مقامات را عقیم بگذارند. گفته می‌شود این تأخیر برروی ۶/۵ میلیون مسافر خارج شهری تأثیر گذاشت و برای راه‌آهن ملی ژاپن بیش از ۶ میلیارد دلار از نظر فروش متوقف شده، خسارت به بار آورد. اکثر کابل‌های آسیب دیده در عرض ۲۴ ساعت تعمیر شدند.[۱۵۰] هدف از این حمله نشان دادن همبستگی با کارگران در حال اعتصاب خطوط آهن بود که نسبت به خصوصی‌سازی برنامه‌ریزی شده در «خطوط آهن ملی ژاپن» اعتراض داشتند. همچنین احتمال داده شد علت این حمله، ایجاد تأخیر در جلسه دادگاه خانم هیروکو ناگاتا، رهبر ارتش سرخ متحد چپگرای افراطی باشد، چراکه وکیل وی به‌علت بروز این خرابی‌ها نتوانست او را به موقع به دادگاه برساند.[۱۵۱]

۲ـ۲ـ ماهواره‌ها و جنگ

ماهواره‌ها نقش اساسی و محوری در جنگ‌های امروزی و به‌خصوص جنگ مبتنی بر شبکه

دارند. ماهواره‌ها نه تنها ستون فقرات اینترنت[1] را ایستاده نگاه می‌دارند، بلکه خود می‌توانند به یکی از ابزارهای عملیات نظامی تبدیل گردند. نیروی هوایی آمریکا در تاریخ ۸ آوریل ۲۰۰۳، یک ماهواره ۸۰۰ میلیون دلاری به مدار زمین پرتاب کرد تا به‌وسیله آن بتواند کلیه اطلاعاتی را که به‌وسیله نظامیان آمریکا مخابره و مبادله می‌شود در سراسر جهان امن سازد. این ماهواره کـه تقریباً ۵ میلیون تن، وزن دارد آخرین ماهواره از ۶ ماهواره از این نوع بود که در منطقـه معینـی در فضا ثابت می‌ماند. این شبکه، ماهواره‌ای شش‌گانه بـه نـام «Mil Star» (مـاهواره مخـابراتی نظامی) پیشرفته‌ترین در نوع خود بوده و ناوها، زیردریایی‌ها، هواپیماها و ایستگاه‌های زمینی را در هر نقطه از جهان به یکدیگر مرتبط نگاه می‌دارند.

یکی از کاربردهای اصلی ماهواره‌ها در جنگ، پیش‌بینی وضعیت هوا است. هواشناسی، یک جزو اساسی در مجموعه عواملی است که تاریخ و چگونگی یـک مأموریـت نظـامی را تعیـین می‌کند.

اطلاعات هواشناسی مورد نیاز آمریکا و انگلیس در جنگ عراق از طریـق گـردان ویـژه ۲۸ عملیاتی در پایگاه نیروی هوایی در کارولینای جنوبی آمریکا تأمین می‌شد. این واحد، بخشی از یک شبکه گسترده و پیچیده پیش‌بینی وضع هوا است که بعد از جنـگ خلـیج‌فـارس در سـال ۱۹۹۱ شروع به‌کار کرد.

اتاق ۱۳۳ در سرفرماندهی گردان هواشناسی واحد عملیاتی با ۲۸ قفـل رمـزی بـاز و بـسته می‌شود. داخل اتاق، نقشه خاورمیانه روی دیوار نصب است و سربازان در لباس خـاکی اسـتتار جنگی در رفت و آمد هستند اما خبرنگاران اجازه ورود به این اتاق را ندارند. این اتـاق، مرکـز سلسله اعصاب هواشناسی فرماندهی کل هوایی ایالات‌متحـده اسـت کـه اختـصاراً CENTAF نامیده می‌شود. «کریس فینتا»[2]، فرمانده هواشناسان در اتـاق ۱۳۳ بـه رادیـو آمریکـا مـی‌گویـد: «واحد ما همه چیز، از گل‌ولای زمین تا خورشید را باید در نظر بگیرد، مثلاً سربازان در جبهـه، ممکن است در گل‌ولای یا خاک گیر کنند. خلبان‌هایی داریم که انواع مأموریت‌ها را باید انجام

1. Back Bone
2. Crease Finta

دهند و وضعیت هوا تأثیر مشخص و متفاوتی بر روی هر کدام دارد. قوای زمینی در عراق باید از وضعیت طوفان خاک و شن و درجه حرارت‌های بالا مطلع شوند، خدمه پرواز نیز باید از وضع تلاطم جوی و ابری باخبر شوند، آنها می‌خواهند درجه و امکان دید را بسنجند»، پیش‌بینی‌های واحد کارولینای جنوبی برای کارشناسان هواشناسی منطقه‌ای در خاورمیانه فرستاده می‌شود. این واحد می‌تواند وضعیت هوا را از یک ساعت تا ۵ روز در یک شعاع ۲/۵ کیلومتر مربع به‌طور دقیق پیش‌بینی کند.

علاوه بر استفاده هواشناسی، ماهواره‌ها برای هدایت مستقیم بمب‌ها و موشک‌های هدایت شونده نیز مورد استفاده قرار می‌گیرند. جنگنده بمب‌افکن‌های آمریکایی در بسیاری از عملیات‌های سرکوب عراق، از این تکنولوژی استفاده کرده‌اند، بمب‌ها در فاصله ۱۲ تا ۳۲۰ کیلومتری هدف رها می‌شوند و هدایت آنها تا اصابت به نقطه هدف، توسط ماهواره‌ها صورت می‌گیرد.

یکی از بمب‌های هدایت شونده MOAB یا همان بمب ۱۰ تنی بود که مخفف Massive Ordnance Air Burst است که Mother of All Battles یا مادر بمب‌ها هم نامیده می‌شود. این بمب از تکنیک GPS یا سیستم جهت‌یابی ماهواره‌ای Global Positioning System استفاده می‌کند. ابزارهای تعیین موقعیت نصب شده بر روی این بمب با فرستادن سیگنال به ده‌ها ماهواره در بالای جوّ، محل دقیق هر نقطه برروی کره زمین را می‌تواند، تعیین کند. «نوع دیگری از بمب‌ها موسوم به E-Bomb است که در این جنگ به کار گرفته شد و فقط می‌توانست مدارهای الکترونیک را از کار بیندازد. این ابزار جنگی که به نام HPM یا «سلاح‌های مایکروویوی مبتنی بر فشار قوی» شناخته شده، نوعی انفجار پرقدرت اما کوته با انرژی الکترومغناطیس ایجاد می‌کند. انفجارهای انرژی الکترومغناطیسی توسط بمب‌های ضعیف یا تفنگ‌های اشعه‌ای قابل حمل به‌وجود می‌آید، برای از کار انداختن یا انهدام وسایل الکترونیکی که کنترل همه چیز از رادارهای دشمن تا کامپیوترها را در اختیار دارند به‌کار برده می‌شود. این سلاح‌ها حتی می‌توانند در کار ابزارها و دستگاه‌های الکترونیکی، نظیر

تنظیم‌کننده‌های ضربان قلب و سایر دستگاه‌های پیشرفته بیمارستان‌ها نیز تأثیرگذاری کرده و آنها را دچار اخلال سازند».[۱۵۲]

۳ـ۲ـ آفت‌های فضای سایبر

آفت‌های فضای سایبر عبارتند از برنامه‌های نرم‌افزاری که اشکال زندگی را تقلید می‌کنند. آنها درست شبیه همتایان خود در دنیای زیست‌شناسی باز تولید می‌شوند (کپی‌هایی از خود تولید می‌کنند) و در اطراف به حرکت در می‌آیند. آنها مانند یک آفت، به‌شدت واگیردار هستند و می‌توانند خسارت‌های قابل ملاحظه‌ای را به وجود آورند. بعضی از آنها مانند بمب‌های ساعتی رفتار می‌کنند و ماهیت واقعی خود را تا زمانی‌که فرصتی برای اشاعه یابند، پنهان نگاه می‌دارند. وقتی که به سیستمی حمله می‌کنند، می‌توانند داده‌ها را خراب کرده یا پاک کنند، در سرویس وقفه ایجاد نمایند، یا داده‌ها را به ایجادکننده خود بفرستند.

این فصل به تشریح دو نوع از آفت‌های فضای سایبر یعنی کرم‌ها و ویروس‌های کامپیوتری می‌پردازد. هر دو آفت، هم کامپیوترها را آلوده می‌کنند و هم از طریق شبکه‌ها گسترش می‌یابند. تفاوت اصلی در اینجا است که کرم یک عامل خودمختار است که کلاً از طریق خودش تکثیر می‌شود، در حالی‌که ویروس، خود را به دیگر نرم‌افزارها می‌چسباند و معمولاً در پاسخ به اقدامات انجام‌شده از طرف کاربران، با آن نرم‌افزار تکثیر می‌شود. همچنین در حالیکه کرم فقط بر روی شبکه‌های کامپیوتری گسترش پیدا می‌کند، اما ویروس می‌تواند از طریق دیسک‌های قابل حمل نیز تکثیر شود. اما تفاوت بین کرم‌ها و ویروس‌ها گیج‌کننده است چراکه رفتار بعضی از آفت‌ها شبیه هر دو است و هر دو نوع آفت، کامپیوترها را آلوده می‌کنند.

آفت‌های سایبر به‌عنوان یکی از ابزارهای جنگ رایانه‌ای باعث خراب شدن یکپارچگی شبکه‌های کامپیوتری و محرومیت از سرویس می‌گردند، حتی اگر عمداً داده‌ها را نابود نکنند یا سیستم‌ها را از کار نیندازند، کامپیوترها باید از خط خارج شده و عملیات متوقف شود تا بتوان آنها را از میان برد.

۴ـ۲ـ ویروس‌ها

ویروس بخشی از کد است که خود را به دیگر دستورات کامپیوتری می‌چسباند؛ از جمله کد برنامه‌های نرم‌افزاری، کد مورد استفاده در بوت کردن کامپیوتر و دستورات ماکرو که در اسناد، کار گذاشته می‌شوند. هرگاه کاربر (یا سیستم) اقدامی انجام دهد که باعث شود میزبان راه بیفتد (مثل روشن کردن کامپیوتر، راه انداختن یکی از برنامه‌های کامپیوتری و یا باز کردن موارد الصاق شده به پیام‌های الکترونیکی)، آن ویروس هم به اجرا درمی‌آید. کد ویروسی به شیوه‌ای به کد میزبان افزوده می‌شود که وقتی میزبان برای اجرا شدن در حافظه load می‌شود، ابتدا ویروس فعال می‌گردد. ویروس اقداماتی را انجام می‌دهد و سپس کنترل میزبان خود را در دست می‌گیرد. ویروس زمانی‌که ویروس فعال شد، می‌تواند یک کپی از خود را در حافظه کامپیوتر ایجاد کند و در همانجا «ساکن» بماند تا اینکه کامپیوتر خاموش شود. این کپی مقیم به دنبال میزبان‌های آلوده نشده می‌گردد، وقتی‌که یکی را پیدا کند یک کپی از خود به درون میزبان تزریق می‌کند. این ویروس ممکن است اقدام به payload کند، یعنی هر کاری انجام دهد، از جمله نشان دادن یک پیام جالب توجه سیاسی، یا پاک کردن فایل‌های موجود بر روی هارد درایو. مثلاً ویروس smiley صورت‌های لبخند زننده را نشان می‌دهد که روی صفحه نمایش به اطراف می‌پرند، اما ویروس میکل‌آنژ، به این اندازه زیرک نیست، چراکه در صورت فعال شدن در تاریخ تولد این هنرمند، یعنی ۶ مارس چند درایو اول هارد دیسک را پاک می‌کند. ویروس Win95/CIH مخرب‌تر است چراکه علاوه بر پاک کردن اولین مگابایت از داده‌های موجود برروی هارد درایو، بخشی از BIOS موجود برروی برخی از تراشه‌های flash ROM را پاک می‌کند. BIOS (سیستم اصلی ورودی و خروجی) برای بوت کردن کامپیوتر مورد نیاز است، بنابراین بوت کردن دوباره با یک دیسک اضطراری نیز امکان‌پذیر نمی‌شود.[۱۵۳] یک شرکت گزارش داد که این ویروس را روی ۸۰ درصد یا حدود ۵۰۰ عدد از کامپیوترهای خود یافته است.[۱۵۴] یک cryptovirus دارای محموله‌ای است که اقدام به رمزگذاری فایل‌ها با یک کلید مخفی می‌کند و موجب می‌شود، محتویات آن برای صاحبانشان

غیرقابل دسترسی شود. این نوع ویروس را می‌توان برای اخاذی نیز مورد استفاده قرار داد.[۱۵۵] فقط حدود ۵ درصد ویروس‌ها حاوی محموله هستند و اکثرشان کاری جزو تکثیر انجام نمی‌دهند. اگر یک ویروس خود را ساکن و مستقر نکند، در این صورت باید میزبان دیگری را آلوده کند و محموله خود را قبل از به‌دست گرفتن کنترل میزبان، آزاد سازد. ویروس‌ها از طریق دیسک‌ها و شبکه‌های کامپیوتری از یک دستگاه به دستگاه‌های دیگر انتقال پیدا می‌کنند.

مفهوم کد تولیدمثل کننده به سال ۱۹۷۰ باز می‌گردد، یعنی زمانی‌که گرگوری بنفورد از اصطلاح «ویروس» برای کدهای ناخواسته کامپیوتری استفاده کرد، آنها می‌توانستند در بین کامپیوترها تولیدمثل کنند و وارد ARPANET (پدر اینترنت کنونی) شوند. دوست بنفورد شخصی به نام دیوید ژرالد، نویسنده داستان‌های علمی ـ تخیلی، این ایده را در رمانی به نام When Harry was One به‌کار برد. اما تا اوایل دهه ۸۰ میلادی طول کشید تا ویروس‌ها را آن‌گونه که امروزه می‌شناسیم، شروع به ظهور کنند و این مفهوم به دست، فرد کوهن که در آن زمان دانشجوی دکترا در دانشگاه کالیفرنیای جنوبی بود به‌صورت رسمی درآمد.[۱۵۶]

کوهن، ویروس کامپیوتری را این‌گونه تعریف کرد: «برنامه‌ای که می‌تواند دیگر برنامه‌ها را با دستکاری آنها «آلوده» کند تا آن برنامه‌ها یک کپی احتمالاً تکامل‌یافته از آنرا دربرگیرند. ویروس با خاصیت آلایندگی خود می‌تواند در سرتاسر یک سیستم کامپیوتری یا شبکه و با استفاده از مجوزهای کاربر گسترش یابد هر برنامه‌ای که دچار آلودگی شود، ممکن است خود نیز همانند یک ویروس عمل کرده و به این ترتیب آلودگی رشد پیدا کند».[۱۵۷]

در اوایل سال ۱۹۹۸ بیش از ۱۳ هزار ویروس کامپیوتری مطرح شدند، هرچند که اکثرشان مشتقات ساده‌ای از یکدیگر بوده و تعداد انگشت‌شماری به‌صورت «وحشی» وجود داشتند ـ یعنی در خارج از یک آزمایشگاه محدود (در باغ وحش). علت تعداد زیاد، شاید این باشد که ویروس‌نویس‌های بالقوه می‌توانند ابزارها و کدهای ویروس‌دار واقعی را از اینترنت یا از دیگر مجاری، پیدا کرده و با آنها کار کنند. در ماه مه سال ۱۹۹۷ گروه Aliance از Digital Hacker اعلام کرد که یک سی‌دی با بیش از ۱۰ هزار ویروس در دسترس عموم قرار گرفته است.

همچنین پیشنهاد کرد که به‌صورت رایگان به ۱۰۰ مشتری اول یک کلکسیون از ۵۰ ابزار ایجاد کننده ویروس، عرضه کنند.(۱۵۸)

کاربرها می‌توانند یک ویروس را از منابع مختلفی «گیر بیندازند» از جمله؛ فلاپی دیسک‌ها[1] و سی‌دی‌ها[2]، موارد الصاق شده به پیام‌های الکترونیکی[3] و صفحات وب که دارای کد جاسازی شده‌ای هستند باید بر روی کامپیوتر کاربر Download شده و به اجرا درآید. معمولاً کاربر باید یک e-mail را باز کند تا ویروس آزاد شود، اما بعضی از سیستم‌های e-mail می‌توانند موارد الصاق شده را به‌صورت خودکار باز کنند.

سه نوع اصلی از ویروس‌ها به نام *برنامه*[4]، *بوت*[5] و *ماکرو*[6] وجود دارند که بر حسب نوع میزبانی که آنها را آلوده می‌کند، نامگذاری شده‌اند. ویروس‌های متعددی دو مورد اول را با هم ترکیب می‌کنند که هم فایل‌های برنامه و هم سکتورهای بوت را آلوده می‌سازند.(۱۵۹)

۵ـ۲ـ ویروس‌های برنامه

ویروس‌های برنامه، فایل‌هایی را آلوده می‌کنند که حاوی کد کامپیوتری هستند، به‌خصوص فایل‌های EXE. و COM. اما فایل‌هایی مانند SYS. و DLL. هم در امان نیستند. هرگاه کاربر، برنامه نرم‌افزاری را فعال می‌کند، آن برنامه، فایل آلوده شده را به اجرا درمی‌آورد و ویروس آزاد می‌شود. مثلاً اگر فایل netscape.exe آلوده شده باشد، هربار که کاربر برنامه Netscape را راه‌اندازی می‌کند، ویروس فعال خواهد شد. ویروس‌های برنامه می‌توانند از طریق هر بستری که برای نقل‌وانتقال نرم‌افزارها مورد استفاده قرار می‌گیرد، گسترش پیدا کنند. از جمله فلاپی دیسک، سی‌دی، موارد الصاق شده به پیام الکترونیکی و download از شبکه. حدود ۸۵

1. Floppy Disk
2. Compact Disk (CD)
3. Attachment to E-Mail
4. Program
5. Boot
6. Macro

درصد از بیش از ده هزار ویروس شناخته شده، جزو ویروس‌های برنامه هستند.(۱۶۰) کم پیش می‌آید که در حالت وحشی باشند.

۶ـ۲ـ ویروس‌های بوت

ویروس بوت، روی سکتور بوت[1] یا دیگر نواحی مرتبط بر روی یک هارد دیسک یا فلاپی تأثیر می‌گذارد. وقتی هارد دیسک یک دستگاه آلوده می‌شود، ویروس را می‌توان در هر بار که دستگاه روشن می‌گردد، فعال کرد. ویروس خود را در حافظه نصب می‌کند و کنترل را به‌دست کد نرمال بوت می‌سپارد. متعاقب آن، ویروس هر فلاپی را که وارد دستگاه می‌شود، آلوده می‌سازد.

ویروس پس از آلوده شدن فلاپی، می‌تواند بر روی کامپیوتر شخصی دیگری گسترس پیدا کند، به شرطی‌که فلاپی آلوده شده در درایو A همان کامپیوتر در زمان روشن شدن قرار داشته باشد (ممکن است دیسک از جلسه قبلی در آنجا جامانده باشد). علت آن این است که وقتی فلاپی در درایو خود باشد، پی‌سی تلاش می‌کند تا کد بوت را از روی یک فلاپی دریافت کند، نه هارد دیسک. اما زمانی‌که کامپیوتر تشخیص می‌دهد که فلاپی دیسک، کد مورد نیاز برای اتمام بوت کردن را ندارد، خیلی دیر شده است. ویروس از همان زمان خود را روی حافظه نشانده و هارد دیسک رآ آلوده کرده است. اما اگر پس از اینکه کامپیوتر بوت کردن خود را تکمیل کرد، یک فلاپی آلوده در آن وارد شود، ویروس هیچ‌گاه فرصت نخواهد داشت تا به اجرا درآمده و هارد دیسک را آلوده کند.(۱۶۱)

یکی از ویروس‌های اولیه‌ای که گزارش شد، یک ویروس بوت نسبتاً بی‌خطر به نام Brain بود. این ویروس در زمانی‌که همراه با تاریخ کپی رایت ۱۹۸۶ مطرح بود، شایع‌ترین ویروس کامپیوترهای شخصی محسوب می‌شد. بنا به اعلام نظرسنجی سالانه سازمان ملی امنیت کامپیوترها در مورد ویروس، تا میانه دهه ۹۰ ویروس Form تبدیل به متداول‌ترین ویروس

---

1. Boot Sector

بوت شده بود. این ویروس اگر ۱۸ ماه فعال می‌شد هربار که یک کلید زده می‌شد، صدای کلیک تولید می‌کرد. در متن درون کد ویروس آمده است: «ویروس Form به هرکس که این متن را می‌خواند، خوشامد می‌گوید. این ویروس، داده‌ها را نابود نمی‌کند، نگران نباشید». اما در واقع این ویروس برای کامپیوترهای جدیدتر، مرگبارتر است، یعنی کامپیوترهایی که اطلاعات دیسک را متفاوت از کامپیوترهای قدیمی که این ویروس برای آن طراحی شده بود، مرتب می‌کنند. نظرسنجی سال ۱۹۹۷ مؤسسه NCSA مشخص ساخت که ۹ مورد از ۱۰ ویروس شایع و ۱۷ مورد از ۲۰ ویروس برتر از نوع ویروس‌های بوت هستند. این ویروس‌ها به‌رغم شیوعی که دارند، فقط ۵ درصد تمام تنش‌های ویروسی را شکل می‌دهند.[۱۶۲]

ویروس میکل‌آنژ، یک ویروس نوع بوت است که به‌نظر می‌رسد گستردگی‌اش پس از یک دوره رشد تنزل یافته باشد. این ویروس در بهار سال ۱۹۹۲ در مطبوعات مورد توجه خاصی قرار گرفت، زیرا تولیدکنندگان و کارشناسان امنیت کامپیوتری نسبت به نوعی اپیدمی احتمالی، هشدار می‌دادند. تاریخ فعال شدن آن یعنی ۶ مارس به سرعت نزدیک می‌شد و کاربران، کپی‌هایی از کد مخرب را بر روی کامپیوترهای شخصی خود می‌یافتند. برخی از افراد، واکنش رسانه‌ها را نوعی هوچی‌گری می‌دانستند، اما این تهدید بیش از حد واقعی بود.[۱۶۳] بنا به گفته کتاب «راهنمای ویروس‌های کامپیوتری» به قلم رابرت اسلید، صدها یا حتی هزاران کامپیوتر شخصی در برخی از مؤسسات آلوده شده بودند و میزان آلودگی در بعضی از مناطق اروپا ۲۵ درصد و بیشتر بود. حداقل ۱۵ شرکت روی دیسک‌های آلوده شده نرم‌افزارهای تجاری عرضه کرده بودند و شرکت Leading Edge ۶ هزار کامپیوتر شخصی را همراه ویروس روانه بازار کرده بود. وقتی ۶ مارس فرا رسید، تعداد اندکی از کامپیوترها در ژاپن نابود شدند، اما برخی باقی ماندند و بدون شک دلیل آن، این بود که بسیاری از افراد، نکات احتیاطی را رعایت می‌کردند. پس از آنکه این ویروس در دانشگاه جورج تاون ردگیری شد، این دانشگاه کد ضدویروس رایگانی را به تمام کاربران ارائه کرد که می‌توانستند در منزل و در سر کار مورد استفاده قرار دهند.[۱۶۴]

۷ـ۲ـ ویروس‌های ماکرو

ویروس ماکرو به‌صورت یک ماکرو auto-exec مطرح است که در فایل‌های سند یک برنامه کامپیوتری همراه با توانمندی ماکرو جاسازی شده است، مانند واژه‌پردازها و برنامه‌های صفحه گسترده[1]. این نوع ماکروها در پاسخ به عملی خاص، مانند باز کردن، بستن یا راه انداختن برنامه‌های کامپیوتری به‌طور خودکار اجرا می‌شوند و زمانی که فعال می‌گردند، کد خود را برروی دیگر اسناد، کپی می‌کنند.(۱۶۵)

ویروس‌های ماکرو عموماً تا قبل از کشف شدن در ژوئیه سال ۱۹۹۵ ناشناخته بودند. در آن سال، ویروسی به نام concept فایل‌های سند Microsoft Word را آلوده کرد، اما هیچ محموله دیگری با خود به همراه نداشت. این ویروس تا پاییز در بین تمام ویروس‌های کامپیوتری بیش از همه گزارش می‌شد. در دو ماه اول سال ۱۹۹۷ ویروس concept تقریباً نیمی از ۳۰۰ سایت مورد نظرسنجی از طرف NCSA را آلوده کرده بود. همچنین حدود $\frac{۲}{۳}$ تمام آلودگی‌های ناشی از ۱۰ ویروس برتر به آن تعلق داشت. مؤسسه NCSA با مقایسه تعداد رویدادهای ویروسی در دو ماه نخست سال ۱۹۹۶ با موارد گزارش شده در سال ۱۹۹۷، اعلام کرد که تعداد آلودگی‌ها با ویروس‌های ماکرو در هر ۱۱۶ روز در حال دو برابر شدن است.(۱۶۶)

از زمان کشف ویروس مذکور، تعداد زیادی از ویروس‌های ماکرو در برنامه word یافت شدند که البته برخی از آنها به‌شدت مخرب هستند. یکی از آنها به نام FormatC می‌تواند فایل‌های موجود برروی هارد دیسک را پاک کند. دیگری با نام Wazzu که در فرم نظرسنجی سال ۱۹۹۷ مؤسسه NCSA در مورد متداول‌ترین ویروس‌ها در مقام دوم قرار گرفت، به‌طور تصادفی، حداکثر سه کلمه را در یک سند به محل‌های مختلف جابجا و رشته حروف«Wazzu» را درج می‌کند. ویروس WM/PolyPoster که در ژوئن سال ۱۹۹۸ کشف شد، تلاش می‌کند تا اسناد Word کاربر را به گروه‌های خبری عمومی ارسال کند. قربانی این ویروس می‌تواند

---

1. spreadsheet

نامه‌های خصوصی یا اسناد انحصاری شرکت خود را به‌صورت منتشر شده برروی اینترنت پیدا کند در حالی‌که همگان مشغول خواندنشان هستند.

در اکتبر سال ۱۹۹۷ اداره ملی فضا و هوانوردی آمریکا (ناسا)[1] مشغول مبارزه با یک ویروس ماکرو شد که از مرکز فضایی جانسون در هیوستون وارد کامپیوترهایی در مسکو شده بود و برای ارتباطات روزمره با خدمه مستقر در ایستگاه فضایی میر، مورد استفاده قرار می‌گرفت. این ویروس که از نرم‌افزار قدیمی ضدویروس عبور کرده بود، کامپیوترهای شخصی (موسوم به pc.) و کامپیوترهای اپل مکینتاش[2] را که برای اتوماسیون اداری و ارتباط با میر به کار می‌رفتند، آلوده کرده بود. این ویروس به ایستگاه میر منتقل نشد، اما طبق گزارش‌ها باعث خرابی پیام‌های e-mail شده بود که به دیوید ولف، فضانورد آمریکایی ارسال شده بود. در حالی‌که مقامات باید ویروس را از سیستم‌های خود حذف می‌کردند باید از به کار بردن موارد الصاقی به پیام‌های الکترونیکی نیز خودداری می‌نمودند.[(۱۶۷)]

ویروس‌های ماکرو از طریق موارد الصاق شده به پیام‌های الکترونیکی، فلاپی دیسک‌ها، اسناد download شده و مرور در وب، وارد سازمان‌ها می‌شوند. معمولاً ویروس از طریق e-mail منتشر نمی‌شود، مگر اینکه فرستنده دانسته یا ندانسته یک فایل آلوده را به پیام خود الصاق کند. ویروس ماکرو، موسوم به Share Fun یک استثنا محسوب می‌شود. وقتی سند آلوده‌شده‌ای باز می‌شود، این ویروس ابتدا global template را آلوده می‌کند تا مطمئن شود سرتاسر سند جدید آلوده شده است، سپس برنامه‌ای را به اجرا درمی‌آورد که آنرا با احتمال یک به چهار به مرحله بعدی می‌رساند. این مرحله بررسی سیستم، برای این هدف انجام می‌گیرد که مشخص گردد، آیا برنامه Microsoft Mail نصب شده است یا خیر. اگر نصب شده باشد، ۳ آدرس پست الکترونیک را به‌طور تصادفی از آدرس پستی کاربر انتخاب می‌کند و برای هر کدام از آنها یک پیام آلوده شده به سند الصاق شده Word ارسال می‌کند. در قسمت موضوع نوشته می‌شود: «شما باید این را بخوانید!» اما در بدنه پیام چیزی نوشته نمی‌شود. با باز

1. NASA
2. Apple Macintosh

شدن موارد الصاق شده، دستگاه گیرنده پیام آلوده می‌شود.[۱۶۸]

ویروس Share Fun شباهت‌های زیادی به یک برنامه قابل اجرای قدیمی‌تر به نام CHRISTMA EXEC دارد. این برنامه که ترکیبی از ویروس، کرم و اسب تروا بود، ابتدا در دسامبر سال ۱۹۸۷ برروی کامپیوترهای mainframe شرکت (آی بی ام) در اروپا (که از طریق شبکه EARN به هم متصل شده بودند) دیده شد. این برنامه، یک پیام الکترونیکی را منتشر می‌کرد که در سیستم PROFS به گردش درمی‌آمد. وقتی پیام آلوده خوانده می‌شد به گیرنده دستور می‌داد: «مرور این پیام به هیچ‌وجه سرگرم کننده نیست. فقط تایپ کنید، کریسمس». انجام این کار، باعث فعال شدن برنامه می‌گشت و به این ترتیب یک درخت کریسمس روی صفحه نمایش ظاهر می‌شد. سپس این برنامه به‌دنبال آدرس‌های e-mail دیگر کاربرانی می‌گشت که پیامی را ارسال کرده یا پیامی را از حساب طرف گیرنده دریافت کرده بودند و به این ترتیب یک کپی از خود را برای آن کاربران می‌فرستاد. سر منشأ کد، دو دانشجو در یکی از دانشگاه‌های آلمان ردیابی شد، اما آنها اعلام کردند، قصد نداشتند هرج‌ومرج به وجود آمده را ایجاد کنند.[۱۶۹]

برنامه CHRISTMA EXEC به این دلیل کرم نامیده شد که برخلاف اکثر ویروس‌ها خود را به کد دیگری متصل نمی‌کند و البته نیازی هم برای این کار ندارد، زیرا یک برنامه خودکفاست. اما به همان اندازه که ویروس است، کرم هم هست زیرا برخلاف دیگر کرم‌ها از طریق پیام‌های e-mail منتشر می‌شود و نیازمند کمک کاربر است. کاربر باید اقدامی را انجام دهد که باعث فعال شدن آن می‌گردد، این برنامه خصوصیات اسب تروا را هم دارد، اما چون اسب‌های تروا لزوماً تکثیر نمی‌شوند به‌نظر می‌رسد این برنامه بیشتر کرم و ویروس باشد تا اسب تروا. آفت مزبور، نشان دهنده کمبودهای موجود در اصطلاح‌شناسی کرم و ویروس است. آفت‌های کامپیوتری را بهتر می‌توان در راستای ابعاد مختلف و مطابق با نکاتی مانند این موارد تعریف کرد که آیا تکثیر می‌شوند یا خیر و اینکه آیا آنهایی که تکثیر می‌شوند با کمک کاربر تکثیر می‌شوند یا به خودی خود و اینکه به چه اجسامی متصل می‌شوند یا نمی‌شوند (فایل‌های قابل اجرا، اسناد، پیام‌های الکترونیکی، سکتورهای بوت و غیره).[۱۷۰]

۸ـ۲ـ تکنیک‌های اختفا[1]

ویروس‌ها از چندین تکنیک برای اختفای حضور خود استفاده می‌کنند. ویروس‌های پنهان، تماس‌های خاصی را در سیستم رهگیری می‌کنند و اطلاعات غلطی را برمی‌گردانند، مانند اندازه یا محتویات یک فایل قبل از اینکه آلوده شود، بنابراین بررسی با اسکنر برای اینکه مشخص شود آیا یک فایل رشد کرده یا دارای کد ویروسی شناخته شده‌ای هست یا خیر، فریب خورده و این تصور ایجاد می‌شود که فایل دستکاری نشده است. ویروس‌های رمزگذاری با ذخیره حجم عمده کد خود به‌صورت به‌رمز درآمده و حضور خود را مخفی می‌کنند. یک روتین رمزگذاری کوچک در ابتدای کد قرار داده می‌شود تا سایر ویروس‌ها در هنگامی‌که فعال می‌شود از رمز درآید. ویروس‌های چند شکلی در زمان تکثیر جهش زیستی پیدا می‌کنند و اسکنرهایی را که دنبال الگوهای ثابتی هستند، فریب می‌دهند. این کار عمدتاً با رمزگذاری انجام می‌شود و هر عنصر جهش‌یافته تحت یک کلید راندوم متفاوت به رمز در می‌آید، به طوری‌که متن‌های رمز آنها کاملاً متفاوت از یکدیگر است. انواع مختلفی از ابزارها، کار ساخت ویروس‌هایی با توانمندی‌های پیشرفته را آسان کرده‌اند. می‌توان یک موتور چند شکلی (polymorphic) مانند Mutating Engine را به هر کد ویروس اضافه کرد تا آنرا تبدیل به ویروس چند شکلی نماید.(۱۷۱)

۹ـ۲ـ چه کسانی ویروس می‌نویسند؟

به‌نظر می‌رسد اکثر ویروس‌های کامپیوتری، کار هکرها باشد. مانند دیگر هکرهای تفریحی، بسیاری از آنها بیشتر انگیزه به مبارزه خواندن و ماجراجویی دارند تا اینکه بخواهند هرج‌ومرج برپا کنند. این امر با درصد نسبتاً اندک ویروس‌هایی که دارای محموله هستند، تأیید می‌شود. جوان ۲۹ ساله‌ای به نام اسپانسکا[2] که با گروه ویروس‌نویس‌های Virus Xchange رابطه چندان مستحکمی نداشت، می‌گوید از «لذت فکری و تجربه رمزآلود و چالش در

---

1. Concealment Tecniques

2. Espanska

برنامه‌نویسی» موجود در نوشتن برنامه ویروس‌ها، لذت می‌برم. همچنین از انجام کاری که تا اندازه‌ای «براندازانه» باشد، لذت می‌برم. نوشتن ویروس با هیجان حضور در محلی تاریک یا انجام کارهای ممنوع یا ترساندن کاربران متوسط همراه است.

یک روز دانشجویی از اندونزی وارد دفتر «دروسی. ای. دنینگ» در جورج تاون شد و بی‌هیچ تعارفی مدعی گشت که نویسنده یکی از دو ویروس سکتور بوت به نام Den Zuk و Ohio می‌باشد. او گفت که آنها را برای لذت فکری نوشته و هیچ کدام از آنها مخرب نیستند. علاوه بر آن، ویروس‌ها اقدام به پاک کردن کپی‌های ویروس Brain کرده بودند، اما این ویروس‌ها «خوش خیم»[1] بودند و هرکس که مورد اصابت یکی از این مهمانان ناخوانده قرار می‌گرفت، می‌دانست که برای خلاص شدن از دست آنها در کامپیوتر یا در کل شبکه کامپیوترهایی که آلوده شده‌اند، چه میزان وقت باید صرف کند.(۱۷۲)

نشانه‌هایی از چند دولت سوءاستفاده کننده از ویروس‌ها به‌عنوان سلاح‌های تهاجمی در جنگ اطلاعاتی در دست است. بنا بر اعلام مرکز مطالعات جنگ‌های زیرساختی، گزارشی در سال ۱۹۹۵ از طرف مؤسسه اطلاعات دفاعی آمریکا هشدار داد که ارتش کوبا، برنامه‌ای در سر دارد تا ویروس‌هایی را برنامه‌نویسی کند که برروی کامپیوترهای غیرنظامی آمریکا تأثیر سوء خواهند داشت. وجود این برنامه از طرف آموری کابالرو[2] مهندس برق که در سال ۱۹۹۲ وارد آمریکا شده و اکنون نیز دستیار موقت استاد در دانشگاه بین‌المللی میامی فلوریدا بود، مورد تأیید قرار گرفت. کابالرو می‌گفت؛ وقتی در دانشگاه هاوانا کار می‌کرده، تیمی متشکل از از ۲۰ نفر در وزارت دفاع با هم ملاقات کردند تا تعیین کنند که چگونه می‌توانند به اهداف خود دست یابند. در گزارش غیر طبقه‌بندی شده ماه مه ۱۹۹۵، مؤسسه اطلاعات دفاعی آمریکا اعلام کرد که قبل از تلاش برای کودتای اوت ۱۹۹۱ در روسیه، سازمان (کا.گ.ب) مشغول نوشتن ویروس‌هایی بوده تا در زمان جنگ یا بحران، سیستم‌ها را از کار بیندازند.(۱۷۳)

---

1. Benign

2. Amori Kabalro

۱۰ـ۲ـ شیوع[1]

در عصر کامپیوتر[2]، ویروس‌ها یکی از بزرگ‌ترین تهدیدات محسوب می‌شوند. از ۱۲۹۰ پاسخ‌دهنده به نظرسنجی سال ۱۹۹۵ مؤسسه Information Week/ Ernst& Young Information Security، ۶۷ درصد شرکت‌ها گزارش دادند که مورد حمله یک ویروس قرار گرفته‌اند. در سال ۱۹۹۶ این میزان، ۶۳ درصد تمام پاسخ دهندگان و ۷۶ درصد هم از افراد شرکت‌هایی بودند که بیش از هزار کارمند دارند. نظرسنجی سال ۱۹۹۶ نشان داد که ویروس‌ها بزرگ‌ترین منبع خسارت مادی هستند (خطاهای غیرعمد در جایگاه دوم قرار دارند). نظرسنجی سال ۱۹۹۷ نشان داد که بیش از نیمی از ۶۴۷ پاسخ دهنده آمریکایی مورد حمله یک ویروس ماکرو قرار گرفته‌اند و ۴۰ درصد آنها خسارت‌هایی تا حداکثر ۱۰۰ هزار دلار گزارش کردند.(۱۷۴)

ویروس‌ها تقریباً متداول‌ترین نوع نقض امنیت هستند که در نظرسنجی ۱۹۹۶ انگلستان به نام «نقض امنیت اطلاعات» گزارش شده‌اند. از ۶۶۱ پاسخ دهنده ۵۱ درصد، مواردی از ویروس را گزارش کردند هرچند که فقط ۵ درصد موارد دارای تأثیر جدی یا قابل ملاحظه‌ای بوده‌اند. ویروس‌ها همچنین مرسوم‌ترین نوع حوادثی بوده‌اند که در نظرسنجی ۱۹۹۸ (اف.بی.ام) به نام «امنیت و جرائم کامپیوتری» ذکر شده بودند.(۱۷۵) تقریباً $\frac{۳}{۴}$ پاسخ دهندگان می‌گفتند که در طول سال گذشته ویروس‌هایی را شناسایی کرده‌اند. در بین افرادی که می‌توانستند کمیت این ضربه را بسنجند، خسارت‌ها از ۵۰ دلار تا ۲ میلیون دلار (که متوسط آن ۵۵ هزار دلار می‌شود) متغیر بودند.(۱۷۶)

نظرسنجی سال ۱۹۹۷ مؤسسه NCSA در مورد شیوع و گستردگی ویروس‌ها نشان داد که عملاً هر ۳۰۰ سایت بررسی شده با یک ویروس مواجه گشته بودند. در ماه فوریه پاسخ دهندگان ۲۵۵۰۰ رویداد را گزارش کردند که از هر هزار کامپیوتر، ۳۳ کامپیوتر را آلوده

---

1. Prevalence
2. In The Computer age

می‌کردند. این مقدار تقریباً دو برابر میزانِ آلودگی گزارش شده در سال ۱۹۹۶ بود. تعداد متوسط رویدادها برای هر سایت ۸۵ مورد بود.(۱۷۷) حدود $\frac{۱}{۳}$ تمام سایت‌ها یک فاجعه ویروسی را در ۱۴ ماه گذشته گزارش دادند که از ۲۹ درصد سال ۱۹۹۶ بیشتر شده بود. بهبود کامل، به‌طور متوسط ۴۴ ساعت و ۲۱/۷ نفر ساعت طول می‌کشید که به‌طور متوسط ۸۳۶۶ دلار هزینه داشت.(۱۷۸) بزرگ‌ترین تأثیر، از دست دادن خلاقیت کاربر از جمله از دست دادن دسترسی به کامپیوترهای شخصی و داده‌ها بود. دیگر اثرات، شامل داده‌های از دست رفته یا خراب شده؛ برنامه‌های غیرقابل اعتماد، پیام‌های روی صفحه نمایش، مداخله، قفل شدن و از کار افتادن سیستم بودند. تقریباً ۴۳ درصد پاسخ‌دهندگان فکر می‌کردند که مشکلات ناشی از ویروس‌های کامپیوتری در سال ۱۹۹۷ بدتر شده‌اند ـ در مقایسه با ۱۹ درصدی که فکر می‌کردند بهتر شده‌اند.(۱۷۹)

منبع آلودگی‌ها عبارت بودند از فلاپی دیسک‌ها (۶۲ درصد بوت و ۳۷ درصد ویروس‌های ماکرو)، موارد الصاق شده به پیام‌های الکترونیکی (۲ درصد بوت و ۳۶ درصد ویروس‌های ماکرو)، موارد دریافت (download) شده (۱۱ درصد بوت و ۹ درصد ویروس‌های ماکرو)، مرور در وب (بوت و ویروس‌های ماکرو هر کدام ۵ درصد) و سایر موارد (۱۹ درصد بوت و ۱۱ درصد ویروس‌های ماکرو).(۱۸۰)

۱۱ـ۲ـ شوخی‌های ویروسی[1]

هشدارهایی درباره ویروس‌های کامپیوتری به شدت مخرب ـ اما کاملاً تقلبی ـ دائماً در اینترنت در گردش و جریان هستند. بسیاری از دریافت کنندگان این پیام‌ها اطلاعات کمی درباره کامپیوترها یا ویروس‌ها دارند، تا متوجه شوند که ویروس‌ها برای سر به سر گذاشتن هستند و در این حد می‌دانند که ویروس‌ها می‌توانند به‌طور بالقوه تمام داده‌های موجود بر

---

1. Virus Hoaxes

روی یک هارد درایو را پاک کنند. متعاقب آن، آنها با حس فرمانبرداری، از دستورالعمل‌ها تبعیت می‌کنند و به هرکس که می‌شناسند، پیام می‌دهند.[۱۸۱]

هشدارهای مربوط به ویروس GoodTimes در اوایل نوامبر سال ۱۹۹۴ در اینترنت به گردش درآمد. این پیام‌ها در ماه سپتامبر از اعتبار ساقط شدند، اما من هنوز آنها را دریافت می‌کنم. در پیام اصلی چنین آمده بود:

«در اینجا اطلاعات مهمی درج شده است. از فایلی به نام Goodtimes بپرهیزید. در شرکت آمریکا آنلاین ویروسی وجود دارد که با e-mail ارسال می‌شود. اگر چیزی به نام GoodTimes دریافت کردید آنرا نخوانید یا download نکنید. این یک ویروس است که باعث پاک شدن هارد درایو شما خواهد شد. این پیام را به دوستان خود ارسال کنید. ممکن است به آنها کمک کند.»[۱۸۲]

بعدها یک نفر در تلاش برای اینکه ادعای خود را معتبر جلوه دهد، اضافه کرد که «کمیسیون فدرال ارتباطات» هشداری را درباره این ویروس منتشر کرده است (در حالی‌که در واقع کار آنها صدور چنین هشدارهایی نیست):

کمیسیون فدرال ارتباطات هشداری را منتشر کرده و نسبت به موضوع بااهمیتی برای کاربران عادی اینترنت اظهار نگرانی کرده است. ظاهراً یک ویروس کامپیوتری جدید به دست یکی از کاربران آمریکن آنلاین AOL مهندسی شده که از نظر توانمندی تخریبی که دارد، بی‌سابقه و بدون رقیب است. دیگر ویروس‌های شناخته شده در مقایسه با ابعاد این موجود جدید که ساخته یک ذهنیت پیچ‌درپیچ است، رنگ می‌بازند. آنچه باعث می‌شود تا این ویروس به این اندازه ترسناک باشد، این حقیقت است که هیچ برنامه‌ای لازم نیست تا مبادله شود و کامپیوتر تازه‌ای را آلوده سازد. این ویروس می‌تواند از طریق سیستم‌های پست الکترونیکی موجود در اینترنت گسترش یابد. وقتی کامپیوتری آلوده می‌شود، یکی از این چندین مورد زیر اتفاق می‌افتد؛ اگر کامپیوتر دارای هارد درایو باشد به احتمال زیاد نابود می‌شود. اگر جلوی این برنامه گرفته نشود، پردازشگر کامپیوتر در یک لوپ باینری نامتناهی قرار می‌گیرد که در

صورت اجرای طولانی می‌تواند به‌شدت به پردازشگر آسیب رساند. متأسفانه برخی از کاربران تازه‌کار کامپیوتر متوجه نخواهند شد که چه اتفاقی در حال وقوع است و زمانی متوجه می‌شوند که دیگر خیلی دیر شده است.[۱۸۳]

موارد متعدد دیگری از سر به سر گذاشتن‌ها نیز وجود دارد. مثلاً روش PENPAL FREETINGS! به کاربران نسبت به یک پیام e-mail هشدار می‌دهد که در صورت خوانده شدن «به‌صورت خودکار خود را به هر شخصی که آدرس پیام الکترونیکی او در صندوق پستی شما وجود دارد، می‌رساند. این ویروس، هارد درایو شما را نابود کرده و این توان بالقوه را دارد تا هارد درایو هر شخص دیگری را که آدرس او در صندوق پستی شما قرار دارد، نابود سازد». این پیام هشدار می‌دهد که خواننده باید «بدون خواندن» هر پیامی که عنوان PENPAL GREETING دارد، آن‌را پاک کند و در خاتمه آمده است «و این پیام را به تمام دوستان و بستگان خود و دیگر خوانندگان در گروه‌های خبری و فهرست‌های پستی که شما عضوشان هستید، برسانید به طوری‌که آنها مورد اصابت این ویروس خطرناک قرار نگیرند!!!»[۱۸۴]

مورد دیگری تحت عنوان Naughty Robot با این جمله آغاز می‌شود، «این پیام از طریق Naughty Robot که عنکبوت اینترنتی است و از طریق روزنه کوچکی در وب جهان‌گستر وارد سرویس دهنده شما می‌شود، ارسال گشته است». این برنامه از یک ضعف امنیتی در HTTP بهره‌برداری می‌کند و به این حالت به سراغ سیستم میزبان شما آمده است تا اطلاعات حساس، شخصی و خصوصی شما را جمع‌آوری کند. این برنامه آدرس ساختمانی و e-mail شما را گردآوری کرده و شماره تلفن و شماره کارت اعتباری شما را می‌داند». به خوانندگان گفته می‌شود تا به مدیر سیستم خود خبر دهند با پلیس تماس بگیرند، تلفن خود را قطع کنند و گزارش دهند که کارت‌های اعتباری خود را گم کرده‌اند.

سر به سر گذاشتن‌های ویروسی، معمولاً با حروف بزرگ و علامت تعجب نوشته می‌شوند تا توجه دیگران را به خود جلب کنند. آنها نسبت به فاجعه‌ای قریب‌الوقوع هشدار می‌دهند، مگر اینکه شخصی فوراً اقدام کند. آنها به خوانندگان خود می‌گویند، این پیام را به هر شخصی

که می‌شناسند، ارسال کنند. پیام، ممکن است شامل اصطلاحات فنی بوده و بعضی از مجوزها را ذکر کند تا آن‌را باورپذیرتر کنند. اما منبع اصلی پیام در اغلب موارد مبهم یا تعیین نشده است، چراکه به یک فرد واقعی نسبت داده نمی‌شود. «اداره مشاوره در حوادث کامپیوتری» که تحت اداره وزارت انرژی آمریکا در آزمایشگاه ملی لاورنس لایومور است، تلاش نموده تا به مردم درباره این نوع سر به سر گذاشتن‌ها و نامه‌های زنجیره‌ای آموزش بدهد.

گروهی از هکرها برای دست انداختن بر روی وب سایتی که هک کرده بودند، یک ویروس منتشر ساختند. در ۸ دسامبر سال ۱۹۹۷ رمزشکن‌ها، وارد سرویسی برای وب سایت معروف یاهو شدند. آنها یک صفحه تقلیدی را که فقط برای کاربرانی مرئی بود که مرورگرشان از فریم‌ها پشتیبانی نمی‌کرد، قرار دادند که در آن آمده بود، هرکس در طول ماه گذشته به یاهو سر زده یک «کرم/ بمب منطقی که در اندرون اعماق کامپیوترشان جاسازی شده»، را دریافت کرده است. این بمب در روز کریسمس ۱۹۹۷ منفجر خواهد شد مگر اینکه کوین میتنیک[۱] از زندان آزاد شود که در آن صورت یک برنامه پادزهر که در کامپیوتری در آمریکای جنوبی وجود دارد، آزاد خواهد شد. این ویروس در کنار سایر موارد «باعث تسریع ساعت‌ها به طرف سال ۲۰۰۰ خواهد شد». در پیام آمده بود که «اتحاد PANTS/ HAGIS کنترل کامپیوترهای دنیا را در دست گرفته است. ما صاحب همه کس و همه چیز هستیم. هیچ‌کس در امان نیست و هیچ کامپیوتری سالم نمی‌ماند. هدف ما سلطه بر دنیا است». این حمله که در ساعت ۷ بعدازظهر به وقوع پیوست به سرعت در سیستم نظارت امنیت یاهو[۲] شناسایی شد و تا ساعت ۷:۱۵ سایت احیا شده بود.(۱۸۵)

موارد متعدد باعث به‌وجود آمدن شوخی‌هایی شده است. یکی هشدار می‌دهد: «مؤسسه تحقیقات در امور پدیده‌های غیرعادی اینترنتی اعلام کرد که بسیاری از کاربران اینترنت به ویروس جدیدی مبتلا شده‌اند که باعث می‌شود، بی هیچ سئوالی، هر قصه بی‌اساس و هشدارهای بی‌مورد را که در مرورگرشان یا در صندوق پستی آنها ظاهر می‌شود، باور کنند».

---

1. Cone Mitnic

2. Yahoo

این پیام، وب سایت‌هایی را درباره افسانه‌های شهری فهرست کرده بود و با این جمله به پایان می‌رسید: «هم‌اکنون این پیام را به همه دوستان خود ارسال کنید. درباره آن فکر نکنید. این داستان به قدری سر موقع است که هیچ تاریخی ندارد و همچنین به قدری بااهمیت است که ما از تعداد زیادی علامت تعجب استفاده می‌کنیم!»

یکی از اولین ویروس‌های شوخی و سر به سر گذاشتن، ویروس مودم ۲۰۰۴ باود بود که در پاییز سال ۱۹۸۸ در اینترنت به گردش درآمد. در پیام آمده بود: «این ویروس خود را روی sub-carrier مودم که در تمام مودم‌های ۲۴۰۰ باود و بالاتر وجود دارد، توزیع می‌کند. مودمی که با این ویروس آلوده شده باشد، ویروس را به مودم دیگری انتقال می‌دهد که در نتیجه از یک sub-carrier استفاده می‌کند». در پیام از طرف شخصی که مدعی بود رابرت تی موریس سوم است (نه همان رابرت تاپان موریس که کرم اینترنت را نوشت) هشداری خنده‌آور مطرح شده بود:(۱۸۶)

«هشدار: ویروس جدیدی آزاد شده که بدتر از هر چیزی است که تاکنون دیده‌ام. این ویروس از طریق سیم برق وارد می‌شود و به سراغ مشترکانی می‌رود که خطوط برق ۶۰ هرتزی دارند. این ویروس با تغییر pinoutهای پورت سریال و با معکوس کردن جهت دوران دیسک کار می‌کند. بیش از ۳۰۰ هزار سیستم فقط در مورفی، داکوتای غربی هدف واقع شده‌اند و این درست در عرض ۱۲ دقیقهٔ گذشته، بوده است».

این ویروس به سیستم‌های RSX-11,Mac,Multics,MVS,VMS,AppleII,Unix,DOS و VHS حمله می‌کند. برای ممانعت از تکثیر این کرم مطالب زیر را جدی بگیرید؛

۱. از سیم برق استفاده نکنید.

۲. از باتری هم استفاده نکنید، زیرا شایعاتی وجود دارد که این ویروس به اکثر کارخانه‌های بزرگ باتری‌سازی حمله کرده و قطب مثبت باتری‌ها را آلوده نموده است.

۳. فایل‌ها را ارسال یا دریافت نکنید.

۴. فایل‌ها را روی فلاپی دیسک یا هارد دیسک ذخیره نکنید.

۵. پیام‌ها را نخوانید. حتی همین پیام را!

۶. از پورت‌های سریال، مودم، یا سیم تلفن استفاده نکنید.

۷. از صفحه کلید، صفحه نمایش یا چاپگر استفاده نکنید.

۸. از سوئیچ‌ها، CPU، حافظه و ریزپردازنده‌ها استفاده نکنید.

۹. از چراغ‌های برق، سیستم تهویه هوای برقی یا گازی، آب لوله‌کشی، آتش، لباس یا چرخ استفاده نکنید.(۱۸۷)

۱۲ـ۲ـ کرم‌ها[1]

کرم برنامه‌ای است که از طریق شبکه کامپیوتری و به‌وسیله نفوذ در کامپیوترها به همان شیوه‌ای که هکر می‌تواند وارد آنها شود از یک کامپیوتر به کامپیوتر دیگر تکثیر می‌شود. آنها برخلاف ویروس‌ها هیچ کمکی از کاربران بی‌حواس نمی‌گیرند. آنها باید کامپیوتری را بیابند که بتوانند نفوذ کنند، حمله‌ای را انجام دهند و کپی خود را برای اجرا شدن به میزبان هدف انتقال دهند. در عمل، یک کرم به‌طور کامل گام‌هایی را که یک متجاوز به سوی کامپیوتر برمی‌دارد و از کامپیوتری به روی کامپیوتر بعدی می‌پرد به‌صورت خودکار درمی‌آورد.(۱۸۸)

بزرگ‌ترین رویداد در تاریخ اینترنت در ۲ نوامبر سال ۱۹۹۸ به وقوع پیوست. رابرت تاپان موریس از دانشجویان فارغ‌التحصیل علوم کامپیوتری در دانشگاه کورنل، برنامه‌ای را معرفی نمود که که چندین کپی از خود تولید کرده و در سرتاسر شبکه پخش می‌کرد. این کرم در عرض چند ساعت به دو تا شش هزار کامپیوتر حمله کرد که این رقم بین ۳ تا ۱۰ درصد کل اینترنت در آن زمان بود. همچنین سیستم‌هایی را که مورد حمله قرار می‌داد، قفل می‌کرد.(۱۸۹) در حالی‌که مدیران سیستم، مشغول پاک کردن این گندکاری بودند، سیستم‌ها می‌بایست از شبکه جدا شده و یا به‌طور کامل خاموش می‌شدند (برخی برای چند روز). وقتی موریس خسارتی را که در حال شکل‌گیری بود، مشاهده کرد از یکی از دوستان خود خواست تا پیامی

---

1. Worms

را در اینترنت منتشر کند و برای از کار انداختن این کار دستورالعمل‌هایی صادر نماید. اما تا آن موقع برای از کار انداختن این آزمایش خیلی دیر شده بود.(۱۹۰) موریس محکوم به نقض قانون کلاهبرداری کامپیوتری و سوءاستفاده از آن شد. وی در ۱۶ ماه مه سال ۱۹۹۰ به مبلغ ده هزار دلار جریمه شد و بابت اقداماتش به سه سال آزادی مشروط و ۴۰۰ ساعت خدمات عمومی محکوم گشت. تخمین خسارت‌ها به‌شدت متغیر بود و نشان می‌داد که به کمیت در آوردن خسارت‌های ناشی از این نوع حمله چه‌اندازه دشوار است. بنا بر اعلام مرکز ملی جرائم کامپیوتری، کلیف استول، ستاره‌شناس و مدیر سیستم‌ها که هکرهای هانوور را ردگیری کرده بود، حداقل ۱۰۰ هزار دلار و حداکثر ۱۰ میلیون دلار خسارت برآورد می‌کرد. جان مک آفی، مدیر شرکت McAfee Associates که محصولات ضدویروس تولید می‌کند، هزینه را بالغ بر ۹۷ میلیون دلار می‌داند.(۱۹۱)

این کرم اینترنتی از برخی روش‌های حملاتی استفاده می‌کرد که مشابه موارد توصیف شده قبلی بودند. مثلاً روی مدل‌های قدیمی برنامه finger daemon اقدام به حمله سرریز بافر می‌کرد. در دمون ارسال پیام سیستم یونیکس از نقیصه‌ای بهره‌برداری کرد که به‌صورت یک فرآیند زمینه[1] برای سروسامان دادن به پیام‌های الکترونیکی در حال ورود کار می‌کند. وقتی دمون ارسال پیام در وضعیت debug مشغول کار بود، این کرم توانست مجموعه‌ای از فرمان‌ها را برای اجرا شدن به او بدهد. این کرم تلاش کرد تا با استفاده از لغت‌نامه ۴۳۲ کلمه‌ای اسم رمزها را بشکند. کلمات موجود در لغت‌نامه برای هر حساب موجود به ترتیب تصادفی مورد استفاده قرار می‌گرفتند.

در طول بحران، دانشمندان کامپیوتر در مؤسسه تکنولوژی ماساچوست[2]، دانشگاه کالیفرنیا در برکلی، دانشگاه پوردو و دیگر سایت‌ها یک تیم واکنش غیررسمی تشکیل دلدند. این دانشمندان، کد این کرم را چند بخش کرده و موارد اصلاحی را منتشر کردند. قبل از پایان ماه،

1. backgroung process
2. Massachusette Institute of Technoloby

مؤسسه پروژه‌های تحقیقاتی دفاعی اقدام به تشکیل مرکز هماهنگ‌سازی تیم واکنش اضطراری کامپیوتری (CERT/CC) کرده بود تا در برابر حملات آینده آماده باشند. از زمان ایجاد کرم اینترنتی به بعد، هیچ حمله واحدی به‌اندازه این سیستم‌ها را از کار نینداخته است.

حدود یک سال پس از این کرم اینترنتی، کرم دیگری کار خود را از طریق شبکه SPAN اداره ملی فضا و هوانوردی آمریکا آغاز کرد. در ۱۶ اکتبر سال ۱۹۹۸ دانشمندانی که به کامپیوترهای موجود در مرکز پرواز فضایی گودارد ناسا واقع در گرین بلت مریلند متصل می‌شدند، یک علامت به‌خصوص لز طرف کرم موسوم به WANK به آنها خوشامد می‌گفت.[۱۹۲]

کرم‌هایی بر ضد قاتلان اتمی

سیستم شما به‌طور رسمی هک شده است.

شما برای همه از دوران صلح حرف می‌زنید، اما برای جنگ آماده می‌شوید.

در زمان حمله، معترضان ضدهسته‌ای در تلاش بودند تا پرتاب شاتلی را که حامل فضاپیمای پژوهشی گالیله بود تا به سیاره مشتری برود، متوقف کنند. سوخت سیستم بوستر ۳۲۵۰۰ پوندی گالیله پلاتونیم رادیواکتیو بود.

یکی از دانشمندان خانم ناسا، پیام‌هایی را از کامپیوتر خود دریافت می‌کرد که خاطرنشان می‌ساختند فایل‌های او در حال حذف شدن هستند (هرچند عملاً حذف نشده بودند). دیگران نیز پیام‌های عجیبی مانند این دریافت می‌کردند: «به یاد داشته باشید. حتی اگر در این مسابقه کثیف، برنده شوید شما هنوز یک موش کثیف هستید» و «به آنارشیست‌ها رأی بدهید». کرم WANK در خارج از شبکه ناسا تا «شبکه جهانی فیزیک پرانرژی» وزارت انرژی به نام HEPNET تکثیر شد. مدیران شبکه فکر می‌کردند پس از دو هفته تلاش‌های شدید، از دست آن خلاص شده‌اند، اما یک مدل جدیدتر و مخرب‌تر ظاهر گشت. دو هفته دیگر طول کشید تا آنرا پاک کنند. جان مک ماهون، مدیر پروتکل در دفتر SPAN ناسا تخمین می‌زند که این کرم برای آنها از نظر هدر رفتن زمان و منابع تا نیم میلیون دلار هزینه داشته است. منبع حمله

هیچ‌گاه کشف نشد، اما برخی مدارک نشان می‌داد که ممکن است از طرف هکرهایی استرالیایی بوده باشد. این کرم از استراتژی‌های حمله ساده‌ای استفاده می‌کرد، مانند امتحان کردن نام کاربری به‌عنوان اسم رمز برای شکستن حساب او.(۱۹۳)

۱۴ـ۲ـ اسب‌های تروا[1]

بنا بر افسانه‌ها، سربازان یونانی که در یک اسب چوبی هدیه شده، پنهان گشته بودند به درون شهر تروا نفوذ کردند. وقتی آنها وارد محوطه شهر شدند، دروازه‌ها را به روی کل ارتش خود باز کردند و تروا را شکست دادند. امروزه اصطلاح اسب تروا برای هر جسمی اطلاق می‌شود که به شیوه‌ای در محدوده یک قلمرو خاص قرار داده می‌شود که ماهیت براندازانده خود را مخفی کند. مثال این قضیه دستگاه ATM (خودپرداز بانک)ترواست که آلن اسکات پیس ۳۰ ساله و جرالد هاروی گرینفیلد ۵۰ ساله در فروشگاه بزرگ باکلند هیلز واقع در منچستر کانتیکات قرار دادند. این ماشین تقلبی برای به‌دست آوردن شماره حساب و PIN مشتریان، بی‌خبر از همه جا کار گذاشته شده بود. گفته می‌شد، جاعلان از اطلاعات مربوط به حساب‌ها برای ساخت کارت‌های تقلبی خودپرداز استفاده کرده و با آنها بیش از صد هزار دلار پول نقد دریافت می‌کردند. پس از اینکه در سال ۱۹۹۳ دستگیر شدند، مقامات کانتیکات متوجه گشتند که نفر اول در نیوهمپشایرّ به‌علت اداره یک فروشگاه جواهرات تقلبی تحت تعقیب است.(۱۹۴)

اسب تروا یکی از ابزارهای جنگ اطلاعات است که برای کسب دسترسی به منابع اطلاعاتی مورد استفاده قرار می‌گیرد. برای یونانی‌ها این منابع همان محوطه فیزیکی شهر تروا بود و برای خلافکارهای کانتیکات این منابع، شماره حساب‌های مشتریان بودند. حضور این اسب، باعث تنزل یکپارچگی محیط اطلاعاتی می‌شود که در آن قرار می‌گیرد. مشتریان بانک فکر می‌کردند که می‌توانند در فروشگاه‌های بزرگ به دستگاه‌های خودپرداز اعتماد داشته باشند، در حالیکه در حقیقت این دستگاه یک وسیله تقلبی بود.

---

1. Trojan Horses

۱۴ـ۲ـ تروا‌های نرم‌افزاری[1]

یک اسب تروای نرم‌افزاری، برنامه‌ای است که وقتی فعال می‌شود، اقداماتی نامطلوب انجام می‌دهد که فرد اجراکننده آن پیش‌بینی نکرده است. می‌تواند فایل‌ها را حذف، یک دیسک را دوباره فرمت[2] و یا داده‌های حساس را تخلیه کند. اگر اجرای کد با یک رویداد عملی شود آن اسب تروا به نام «بمب منطقی»[3] و یا در صورتی‌که با ساعت معینی فعال شود به نام «بمب ساعتی»[4] خوانده می‌شود. کد مخرب[5] معمولاً درون یکی از برنامه‌های سیستم مخفی می‌شود که اگر جذاب هم نباشد، حداقل به‌نظر معصوم می‌رسد و عملاً می‌توان آنرا در هر برنامه‌ای مستقر کرد، از جمله یک واژه‌پرداز، برنامه‌های صفحه گسترده[6]، بازی‌های کامپیوتری، برنامه‌های مالی یا تجهیزات سیستم. مدل ترواپی را می‌توان از طریق پیام الکترونیکی توزیع کرد یا روی وب منتشر نمود. کاربران ناغافل می‌توانند با باز کردن ضمیمه یک پیام الکترونیکی یا دریافت نرم‌افزار از وب آنرا به‌دست آورند.

در برخی از موارد، کد تروا به‌دست خودی‌ها روی سیستم نصب می‌شود. مایکل لافنبرگر، قبل از ترک شغل خود در شرکت General Dynamics یک بمب منطقی از خود بر جای گذاشت تا یک برنامه کامپیوتری را که خودش برای ردیابی قیمت‌ها و در دسترس بودن قطعات برای موشک‌های اطلس نوشته بود، نابود کند. او این اسب تروا را به‌عنوان برنامه‌ای به اسم Cleanup مخفی کرده بود و طوری طراحی شده بود که پس از پاک کردن قسمت‌هایی از برنامه، خود را پاک کند. نقشه او زمانی ناکام ماند که یک تکنیسین با مأموریت رفع اشکالات، بمب را کشف کرد. بنا بر مندرجات حکم تعقیب در دادگاه فدرال سان‌دیه‌گو، او فکر می‌کرد که می‌تواند با ترک این شرکت و استخدام به‌عنوان یک مشاور برای دوباره‌سازی برنامه قطعات، پول بیشتری کسب کند. هدف این بمب منطقی، تضمین این نکته بود که شرکت به

---

1. Spftwaretrojans
2. Format
3. Logic Bomb
4. Time Bomb
5. Malicious Code
6. spreadsheet

خدمات او نیاز خواهد داشت. برنامه Cleanup قبل از زمان برنامه‌ریزی شده خود از کار افتاد.(۱۹۵)

هکرها با قرار دادن یک اسب تروا که ظاهری طبیعی دارد، اما در پشت صحنه مشغول سرقت اسم رمز کاربران بی‌خبر است به جای یک برنامه استاندارد login روی یک کامپیوتر، توانستند اسم رمزها را به‌دست آورند. پس از اینکه کاربران نام کاربری و اسم رمز خود را تایپ می‌کنند، برنامه مقادیر موجود در یک فایل را دور می‌ریزد و پیام از کار افتادن برنامه را نشان داده و سپس کنترل را به برنامه login واقعی که به‌طور عادی اجرا می‌شود، انتقال می‌دهند. چون اسم رمزها در زمان login چاپ نمی‌شوند، کاربران به این نتیجه می‌رسند که اشتباه کرده‌اند و بنابراین اعداد را در واکنش به درخواست دوم دوباره تایپ می‌کنند. اگر یک برنامه login از نوع تروایی به دستگاه من حمله کند، در اینجا چیزی که ظاهر خواهد شد، ذکر گشته است:

Login: **denning**
Password:
Iogin incirrect
Iogin: **denning**
Password
Last login: Thu Aug 7 08:43:11 from guvax

مدتی بعد، هکر می‌تواند به فایل دسترسی داشته باشد و اسم رمزها را بازیابی کند. با چنین برنامه‌ای ممکن است یک خودی یا متجاوز تلاش کرده تا فقط یک حساب را با امتیاز محدود به خطر بیندازد تا بتواند یک اسم رمز ریشه‌ای را به‌دست آورد.

در حالیکه کلیف استول[1] بر کار یک هکر آلمانی نظارت داشت، دید که این متجاوز اقدام به انتقال یک برنامه login تروایی به درون کامپیوتر او کرده است. استول که نمی‌خواست خود را نشان بدهد، یک خط را در برنامه تغییر داد و کاری کرد که به‌نظر برسد، هکر اشتباه کوچکی مرتکب شده است. همچنین یکی دو تا از پارامترهای سیستم را پیچاند تا سرعت سیستم کند

1. Cliff Stoll

شود. این هکر، برنامه را دوباره ساخت، اما آنرا در دایرکتوری اشتباهی نصب کرد و در آنجا بیکار ماند. در اینجا، این برنامه نوشته شده است:

سه گزاره "echo" اول یک خوشامدگویی را برروی صفحه نمایش ظاهر کرده و سپس از کاربر یک نام حساب (account name) درخواست می‌کند. اسکریپت پس از خواندن نام حساب و مطرح کردن یک اسم رمز این اکو را غیرفعال می‌کند (stty-echo) در حالیکه کاربر مشغول تایپ یک اسم رمز است. بنابراین هرچه کاربر تایپ کند، روی صفحه نمایش ظاهر نمی‌شود. اکو دوباره فعال می‌شود و این اسکریپت از آن برای وارد کردن اسم رمز و نام حساب تایپ شده به‌دست کاربر به درون یک فایل به نام "pub" در دایرکتوری "/tmp" استفاده می‌کند. سپس به کاربر گفته می‌شود که login موفق نبوده و در این مرحله برنامه login اصلی کنترل را به‌دست می‌گیرد.

دانشجویان، برنامه‌های login تروایی را در حال اجرا بر روی کامپیوترهای موجود در آزمایشگاه دانشکده به حال خود رها می‌کنند. به این ترتیب لازم نیست، سیستم عامل را از کار بیندازند و برنامه login استاندارد را جایگزین کنند. در عوض، آنها صرفاً برنامه خود را راه می‌اندازند و سپس از کامپیوتر دور می‌شوند. کاربرانی که به کامپیوتر نزدیک می‌شوند، فکر می‌کنند که برنامه استاندارد در حال اجراست. تنها راه برای پرهیز از این دام، بوت کردن دوباره سیستم است.

کن تامپسون[1]، یکی از همکاران نویسنده سیستم یونیکس در شرکت Bell Labs، در سخنرانی خود به نام ACM Turing توضیح داد که چگونه می‌توان یک اسب تروای قدرتمند ساخت که به نویسنده خود امکان دهد تا به هر حساب با کمک اسم رمز اختصاص داده شده به آن حساب یا اسم رمزی که نویسنده انتخاب کرده است، وصل (log on) شود. بمب login تامپسون دارای این خاصیت جانبی بود که در کد مبدأ login غیرقابل شناسایی باشد. در حقیقت، این بمب به هیچ عنوان در کد مبدأ قرار نمی‌گیرد و به جای آن کامپایلر موجود برای

1. Ken Thompson

زبان برنامه‌نویسی طوری دستکاری می‌شود که بتواند اسب تروا را به درون object code قابل اجرای برنامه بفرستد.(۱۹۶)

در دانشگاه جورج میسون فردی در فوریه سال ۱۹۹۷ اقدام به نصب اسب تروا در سرویس دهنده site.gmu.edu کرد. بنابراین هرگاه که شخصی برنامه Netscape Navigator را فعال می‌کرد قبل از آنکه کنترل در اختیار این مرورگر استاندارد وب قرار گیرد، به طور پنهانی یک پیام الکترونیک صادر می‌کرد. این پیام که از حساب کاربر فرستاده می‌شد اعتراضی یک سطری خطاب به حساب STOPIT دانشگاه بود که برای برقراری ارتباط با Security Review Panel به کار می‌رفت. این حمله پس از تولید حدود ۱۰۰ پیام، زمانی کشف شد که دانشجویان گزارش دادند از STOPIT برای شکایت‌هایی که نفرستاده‌اند، پاسخ‌های اتوماتیک دریافت می‌کنند. بازرسان دانشگاه فکر می‌کردند که این حملات از طرف یکی از دانشجویان سابقی باشد که حسابش چند روز قبل به عنوان بخشی از یک خانه‌تکانی روزمره برای حذف حساب‌های دانشجویانی که دانشگاه را ترک کرده بودند، لغو شده بود. این دانشجو، بابت نقض خط‌مشی دانشگاه در استفاده از کامپیوتر چندین اخطار اداری دریافت کرده بود. این حمله متعاقب رویدادهای دیگری نیز به وقوع پیوست که در طی آن، هکرها به کامپیوترهای دانشگاه دسترسی پیدا کرده و از آنها برای نفوذ به دیگر سیستم‌ها استفاده می‌کردند. اتهامات رسمی علیه دو نفر از دانشجویان تنظیم شد، اما در دادگاه فیرفکس نقض شدند. مدرک اصلی یعنی فایل‌های e-mail از طرف قاضی، موثق قلمداد نشد، زیرا هیچ‌کس نمی‌توانست اثبات کند که پیام‌ها اصل هستند. حتی اگر مدارک از نظر قانونی قابل قبول بودند، این سؤال مطرح می‌شد که آیا پرونده منتهی به یک محکومیت می‌گردد یا خیر؟(۱۹۷)

یکی از شرکت‌های نرم‌افزاری به نام "Cadsoft" از یک اسب تروا برای قرار دادن دام بر ضد تکثیرکنندگان قاچاقی نرم‌افزار استفاده کرد. این شرکت یک برنامه رایگان[1] به نمایش گذارد که دیسک را برای کپی‌های دزدی شده از نرم‌افزارهایش جست‌وجو می‌کرد و اگر

1. Free Program

موردی پیدا می‌شد، برنامه یک حواله چاپ می‌کرد که به شرکت مورد نظر امکان می‌داد در ازای یک هندبوک[1] رایگان پست کرد. شرکت Cadfast به ۴۰۰ کپی کننده قاچاقی که پاسخ داده بودند، نامه‌هایی فرستاد و درخواست پرداختی معادل حداقل ۶ هزار مارک آلمان را کرد. در چنین حالتی، اسب تروا در حکم یکی از ابزارهای دفاعی جنگ اطلاعات عمل کرد.(۱۹۸)

شرکتی با آدرس پاناما به نام "PC Cyborg" کاری بیش از یک مخرب انجام داد. آنها ۱۰ هزار کپی از بسته موسوم به «اطلاعات ایدز»[2] همراه با یک توافق صدور مجوز غیرمعمول توزیع کردند که به کاربران هشدار می‌داد، مکانیسم‌های مخصوص این برنامه اگر از شرایط این توافق‌نامه تبعیت نکنند، روی دیگر نرم‌افزارهای موجود برروی سیستم آنها تأثیر نامناسبی خواهد گذاشت. زمانی که این برنامه نصب می‌شد، تعداد دفعاتی را که کامپیوتر دوباره بوت می‌شد، می‌شمرد. پس از ۹۰ بار بوت مجدد، هارد دیسک[3] را رمزگذاری می‌کرد و صورت حسابی به کاربر نشان می‌داد و درخواست می‌کرد تا در ازای کلید این رمز، هزینه این مجوز را بپردازد. مقامات، چهار مدیر و یک همدست آمریکایی را در پشت این اقدام شناسایی کردند.(۱۹۹)

در نوامبر سال ۱۹۹۵ شرکت آمریکن آنلاین به کاربران خود نسبت به یک اسب تروا هشدار داد که از طریق پیام الکترونیکی به نام AOLGold یا install.exe منتشر می‌شد. اگر موارد الصاق شده به پیام، باز و اجرا می‌شدند، می‌توانست سبب خرابی هارد درایو گردد. در عرض کمتر از دو سال بعد، شرکت AOL و سازمان ملی امنیت کامپیوتر به کاربران AOL نسبت به اسب‌های تروای دیگری که ازطریق e-mail در گردش بودند، هشدار داد. فایل الصاق شده به محض باز شدن، برنامه‌ای را آزاد می‌کرد که مخفیانه اسم رمز و نام حساب مشترکان را جمع‌آوری می‌کرد و آنها را به نویسنده برنامه باز می‌گرداند. مدل‌های مختلف و متعددی از این فایل وجود داشتند و AOL به کاربران خود هشدار می‌داد که هیچ چیزی را که

1. Hand Book
2. Aides Information
3. Hard Disk

به zip. یا exe. یا scr. ختم می‌شوند، باز نکنند، زیرا تمام آنها می‌توانند، حاوی کد قابل اجرا باشند.[۲۰۰] پیام‌ها همگی با یک ظاهرسازی و بعضی با ارائه مطالب هرزه‌نگارانه و سایرین به صورت برنامه‌هایی برای تقویت چاپگر، مودم یا نرم‌افزارهای AOL می‌آمدند.[۲۰۱] برخی از اسامی فایل‌ها به صورت aol31.exe یا games.exe یا porn.zip بودند. در ماه ژوئن سال ۱۹۹۸ جوانی در نیویورک، بابت سرقت بیش از ۵۰۰ اسم رمز از کاربران AOL و با کمک اسب تروا خود محکوم شد.[۲۰۲]

در کل، امکان ندارد اسب تروایی تهیه شود که فقط متن اصلی یک پیام را بخواند. اما گفته می‌شود برخی از سیستم‌های پست الکترونیکی، کنترل‌های ActiveX و Java appletهای جاسازی شده را به طور خودکار باز و فعال می‌کنند و این امکان را می‌دهد تا کاربران در حال خواندن پیام‌ها را با این نوع کدها مورد اصابت قرار داد.[۲۰۳]

۱۵ـ۲ـ سواری در وب[1]

وب، مکانیسم انتقال قدرتمندی برای نرم‌افزار و اسب‌های تروا دارد. کاربران با کلیک ماوس می‌توانند برنامه‌های کامل را دریافت (download) کرده و یا به بسته‌های موجود ارتقا پیدا کنند. در دسامبر سال ۱۹۹۶ و تا اواسط ماه ژانویه، کاربران حداکثر ۳ هزار دلار در نقشه‌ای را از دست دادند که از طریق وب سایت‌های هرزه‌نگار به نام sexygirl.com و ladult.com و beavisbutthead.com طراحی شده بود. به بازدیدکنندگان گفته می‌شد که برای مشاهدهٔ عکس‌های برهنه لازم است یک برنامه مخصوص برای دیدن عکس داشته باشند و این برنامه را می‌توان با کلیک برروی یک لینک به دست آورد. وقتی این اسب تروا download می‌شد، صدا را از روی مودم کاربر قطع می‌کرد و آنرا از شرکت محلی ارائه‌دهنده خدمات اینترنتی جدا کرده و دوباره به یک شماره تلفن در مولداوی متصل می‌نمود (مولداوی در شوروی سابق قرار دارد.) این تماس به وسیله یک کامپیوتر پاسخ داده می‌شد که کاربر را دوباره به وب

1. Riding the Web

سایت اولیه متصل می‌کرد. (کامپیوتر مذکور عملاً در کانادا قرار داشت، اما هزینه‌ها با نرخ مولداوی محاسبه می‌شدند.) کاربر در نهایت عکسی را که انتظار داشت به دست می‌آورد، اما بعدها یک صورت حساب سنگین تلفن دریافت می‌کرد. حتی زمانی که کاربر ارتباط خود با اینترنت را قطع می‌کرد، اسب مولداوی خط تلفن را آزاد نگه می‌داشت و هزینه‌ای معادل ۲ دلار در دقیقه صادر می‌کرد. این تماس تا زمانی که مودم یا کامپیوتر را خاموش نمی‌کردند به پایان نمی‌رسید.[۲۰۴]

بنا بر اعلام مقامات، درست در عرض ۶ هفته ۸۰۰ هزار دقیقه از زمان تماس به مولداوی جمع شد. کمیسیون تجارت فدرال در ماه ژانویه اقدام به انجام تحقیقاتی کرد و در نهایت به مقامات حاضر در وب‌سایت‌های دارای کد تروا رسیدند. در عرض یک ماه این کمیسیون، سایت‌ها را تعطیل کرد و علیه ۳ نفر در لانگ آیلند در نیویورک که گفته می‌شد مرتکب این کلاهبرداری شده‌اند، تشکیل پرونده داد. در ماه نوامبر کمیسیون مزبور اعلام کرد که با افراد و شرکت‌های درگیر به توافقاتی دست یافته است. این توافقات، شامل ۲/۷۴ میلیون دلار بازگرداندن هرینه به ۳۸ هزار مشتری بود که دچار ضرر بسیاری شده بودند. شرکت‌های نامبرده در این توافقات عبارت بودند از:

Auditex Connectionm, Promo Line, Internet Girls, NiteLine Media

با تروای مولداوی، کاربران مجبور بودند به صراحت درخواست کنند که نرم‌افزار مورد نظر روی سیستم آنها download شود. دیگر انواع تروا‌های مبتنی بر وب به این آسانی قابل اجتناب نیستند. آنها می‌توانند در برنامه‌ها کمین کنند و به طور اتوماتیک زمانی که کاربر روی یک لینک کلیک می‌کند تا به صفحه دیگری در وب برود download شده و فعال شوند. این توانمندی به توسعه دهندگان وب سایت‌ها امکان می‌دهد تا به‌جای یک صفحه نمایش پر از متن و عکس، به کاربران تجربه‌ای پویا دهند، اما این امر، کاربران را در معرض خطر بزرگ‌تری قرار می‌دهد.

اعضای گروه Chaos Computer Club در هامبورگ آلمان نشان دادند که چگونه اسب

تروای انتقال یافته در وب می‌تواند پول را از یک حساب بانکی تخلیه کند. برنامه آنها از ActiveX استفاده می‌شد، برنامه‌ای که شرکت مایکروسافت برای مرورگر وب خود به نام Internet Explorer برنامه‌نویسی کرده است. وقتی کاربر روی یک لینک منتهی به برنامه کامپیوتری ActiveX کلیک می‌کند سند یا شیئی همراه با کد دریافت می‌شود و روی کامپیوتر فرد کاربر به اجرا در می‌آید. تروای گروه فوق، کامپیوتر کاربر را به دنبال برنامه Quicken که یک برنامه کامپیوتری مالی و دارای توانایی در انتقال پول است، اسکن می‌کند. اگر برنامه یادشده پیدا می‌شد، جزئیاتی را درباره حساب‌های بانکی کاربر استخراج می‌کرد و معامله‌ای تقلبی شکل می‌گرفت تا پول از حساب فرد کاربر به حساب نفر دیگری انتقال داده شود. این معامله که از نگاه کاربر دور می‌ماند و در یک فایل سفارش‌های انتقال قریب‌الوقوع ذخیره می‌شد، دفعه بعد که برنامه Quicken به سرویس بانکداری آنلاین متصل می‌شد، اجرا می‌گشت.[۲۰۵]

در ۳ آوریل سال ۱۹۹۷، مایک ماتسومورا از مهندسان JavaSoft در شرکت سان میکروسیستمز طرز کار یک اسب تروای وب را که به دست فرد مک لین (نویسنده برنامه اصلی Internet Explorer) نوشته شده بود، نشان داد. این برنامه باعث می‌شد تا کامپیوتر کاربرانی که از صفحه وب آن بازدید می‌کردند از کار بیفتد. آخرین ساخته مک لین که وب سایتی بود به نام Outer Limits بود که حاوی یک برنامه ActiveX است که به محض download شدن، یک دموی چند رسانه‌ای پخش می‌کرد و با در دست گرفتن کنترل صفحه کلید، یک دیسک را فرمت کرده و پس از به راه انداختن برنامه Quicken اقدام به بررسی اطلاعات دفترچه‌های چک می‌کرد و در نهایت سوابق مالیاتی کاربر را نشان می‌داد. این دموی ActiveX بخشی از سخنرانی ارائه شده از طرف رئیس شرکت سان و اسکات مک لی در کنفرانس موسوم به JavaOne در سان فرانسیسکو بود. مک‌لی با این فرمول به توصیف ActiveX پرداخت:

ActiveX= Java+ Porting+ Memory+ Leaks+ Viruses

وی سپس با تأکید بر اهمیت امنیت، سخنان خود را به پایان رساند.[۲۰۶]

همچنین در ماه آوریل شرکت McAfee Associates اعلام کرد که نقصی را در ترکیبی از ویندوز ۹۵، Internet Explorer 3.x و Norton Utilities 2.0 پیدا کرده‌اند که بـه اسـکریپت صفحه وب حساس به ActiveX امکان می‌دهد تا هر یک از برنامه‌های کامپیوتری را بـه اجـرا در آورد. یک اسکریپت مخرب می‌تواند هارد دیسک کاربر را فرمت کرده یا از پروتکل انتقـال فایل (FTP) اسـتفاده کنـد تـا اسـناد حـساس را از دسـتگاه کـاربر بـه سـرقت ببـرد. شـرکت Symantec فوراً با رفع نقیصه در برنامه نورتن از خود واکنش نشان داد.[۲۰۷]

با وجودی که مشکلات در مقایسه با آنهایی که با ActiveX برخـورد داشـتند، کمتـر حـاد بوده، اما در مورد Java متعلق به شرکت سان، مواردی از نقـاط ضـعف گـزارش شـده اسـت. Java که از محیط‌ها و زبان‌های برنامه‌نویسی است به برنامـه‌نویـسان وب امکـان مـی‌دهـد تـا برنامه‌هایی را به نام Java applet بنویسند که در مرورگـر وب کـاربر download شـده و بـه اجرا در می‌آیند. این امر، مورد حمایت مرورگر شرکت سان بـه نـام Hot Java و مرورگرهـای Netscape Navigator و Internet Explorer است. محققان دانشگاه پرینستون چندین مـورد از نقاط ضعف امنیتی را در انواع نسخه‌های عرضه شده مرورگرها یافته‌اند که بـه یـک applet تروایی امکان می‌دهند تا کامپیوتر کاربر را قفل و سرویس را تضعیف کنند، اطلاعـات موجـود در دستگاه کاربر را به طرف دیگری درز بدهند و فایل‌هایی را کـه مـورد اسـتفاده برنامـه‌هـای کامپیوتری دیگری هستند خراب کنند. شرکت سـان، گـام‌هـایی را بـرای رفـع ایـن مـشکلات برداشته و امنیت محیط Java را تقویت کرده است.[۲۰۸]

مشکلات امنیتی در Java Script نیز پدید آمده‌اند. این یک زبان برنامه‌نویسی می‌باشـد کـه در شرکت Netscape Communications برای Navigator برنامه‌نویسی شـده اسـت. جـاوا اسکریپت که هیچ ارتباطی با جاوا ندارد، مورد حمایت Internet Explorer نیز اسـت. نقـصی که در ژوئیه سال ۱۹۹۷ گزارش شده بود به برنامه‌نویس صفحه وب اجازه می‌داد تا کـد جـاوا اسکریپت را که فعال کننده یک اسب تروا در مرورگر کاربران بی‌خبر از همه جاست، بنویـسد.

این برنامه سرکش می‌تواند تمام داده‌هایی را که کاربر در یک فرم تایپ کرده است، از جمله شماره کارت اعتباری و کلیدواژه‌های جست‌وجو را بخواند.(۲۰۹)

نقاط ضعف متعدد دیگری نیز در مرورگرهای وب کشف شده‌اند که ناشی از توانمندی آنها در اجرای فرمان‌هایی است که از طرف یک سایت دور دست داده شده است. در ماه مارس ۱۹۹۷ مشکلی در Internet Explorer گزارش شد که به برنامه‌نویسان صفحات وب امکان می‌داد تا در خفا برنامه‌های ذخیره شده برروی کامپیوترهای شخصی کاربران را به اجرا در بیاورند. وقتی کاربر روی یک لینک موجود در صفحه‌ای با اسب تروا کلیک می‌کرد. آن لینک به میانبر (shortcut) ویندور ۹۵ یا (ان تی) که برای راه انداختن یک برنامه کامپیوتری مورد استفاده قرار می‌گیرد، متصل می‌شد. ایجاد کننده صفحه وب[1] برای سوءاستفاده کردن باید بتواند محل دقیق میانبر را در دایرکتوری فایل‌های کاربر[2] حدس بزند تا آنرا در لینک به رمز در آورد. چون بسیاری از برنامه‌ها در محل‌های استاندارد ذخیره می‌شوند، این کار خیلی هم سخت نیست و بنابراین شرکت میکروسافت سریعاً اعلام کرد که این نقص برطرف شده است.

در اکتبر سال ۱۹۹۷ میکروسافت[3] گزارش داد، برای مشکلی که یکی از مشاوران آلمانی به نام رالف هاوسکس، کشف کرده است، در عرض ۲۴ ساعت، رفع عیب منتشر خواهد کرد. هاوسکس که برای یک مجله کامپیوتری به نام C't برنامه Internet Explorer 4.0 را بررسی کرده بود، متوجه شد که یک برنامه‌نویس بدخواه صفحات وب می‌تواند به انواع خاصی از فایل‌ها بر روی هارد دیسک هر کاربر دسترسی داشته باشد. فرد متجاوز باید نام دقیق فایل و دایرکتوری را که این فایل در آن قرار دارد، بداند. اما حتی شبکه شرکت‌های تحت حفاظت یک دیواره آتش نیز در برابر این حمله آسیب‌پذیرند.(۲۱۰)

فرد متجاوز برای استقرار اسب تروا، فرمان‌هایی را برای آوردن فایل مورد نظر در داخل یک سند HTML مخفی می‌کند. وقتی کسی به صفحه وب مورد نظر سر می‌زند این فایل بر

---

1 The Creator of the Web Page
2. User's File Directory
3 Microsoft

روی کامپیوتر او download می‌شود. در آن زمان، مرورگر شرکت میکروسافت فرمان‌ها را اجرا می‌کند و این فرمان‌ها فایل مورد نظر را آلوده و به سرویس دهنده فرد متجاوز می‌فرستد. این حمله را می‌توان با فرستادن ترواي HTML به قربانی مورد نظر از طریق پیام الکترونیک آغاز کرد. بنا بر اعلام مدیر تولید IE4.0 در میکروسافت به نام کوین یونانگست، کاربران می‌توانند با پیکره‌بندی Security Zone در این برنامه برای از کار انداختن اسکریپتینگ سایت‌های ناآشنا از این دام بپرهیزند.(۲۱۱)

محققان دانشگاه پرینستون نشان دادند که چگونه می‌توان کل وب را در یک con game بزرگ تقلید کرد. مهاجمان پس از کشاندن فردی به سرویس دهنده وب خود، آن فرد را در سایت خود نگاه می‌دارند و در همان حال یک مدل تقلبی از وب را به کاربر نشان می‌دهند. در تمام این مدت، فرد قربانی از این ترفند بی‌خبر است. برای وسوسه فردی به طرف این بازی، مهاجمان می‌توانند یک لینک را روی سرویس‌دهنده وب خود به طرف صفحه‌ای قرار دهند که فرد مورد نظر به آن سر می‌زند. به این ترتیب ممکن است آنها آدرس صفحه وب را به نام Uniform Resource Locator با یک پیام پستی به فرد مورد نظر در یک پیام وسوسه کننده بفرستند. هرگاه قربانی یک فرم را پر می‌کند، محتویات قبل از آنکه به سرویس دهنده واقعی فرستاده شوند، بررسی می‌گردند. این برنامه، اسم رمزها، شماره کارت اعتباری و دیگر اطلاعات حساس را رد می‌کند.(۲۱۲)

۱۶ـ۲ـ رله پیام الکترونیکی[1]

رله پیام الکترونیکی عبارت است از یک سرویس اینترنتی که اقدام به معرفی حساب‌های پست الکترونیکی دائم به کاربرانی می‌کند که حساب‌های شخصی یا شغلشان در معرض تغییر قرار دارد. مشترکان می‌توانند حساب رله خود را برروی کارت‌های تجاری پرینت کنند و در همان حال، حساب را طوری تنظیم کنند که تمام پیام‌های الکترونیکی در حال ورود را، به

1. E-mail Relays

حساب‌های عادی آنها بفرستند، یعنی جایی که خوانده شده و پردازش می‌شوند. مزیت چنین کاری برای مشتریان این است که آنها می‌توانند یک آدرس e-mail دائم را حتی وقتی که شغل یا شرکت ارائه دهنده خدمات اینترنتی خود را تغییر می‌دهند، اعلام کنند و نقص آن این است که ارائه دهنده رله e-mail این توانایی را دارد که در تمام پیام‌های در حال عبور از طریق رله، استراق سمع کند.

با وجودی که هیچ رویداد گزارش شده‌ای از این نوع رله‌های تروایی وجود نداشته، اما در اکتبر سال ۱۹۹۷ تیم واکنش اضطراری کامپیوتری نیروی هوایی توصیه‌نامه‌ای را منتشر کرد که یک شرکت در هلند برای سرویس رله e-mail خود در حال هدفگیری کاربران نظامی است. شرکت Milmail به کاربران، آدرس‌های e-mail را پیشنهاد می‌کرد که دارای نام قلمرویی با ظاهر نظامی بودند، مانند AirForce.net یا F16.AirForce.net. پیام‌های الکترونیکی ارسال شده به یکی از آدرس‌های این شرکت به طور خودکار به حساب عادی e-mail کامپیوتر ارسال می‌شد. این نوع رله کردن می‌توانست اطلاعات قابل ملاحظه‌ای را درباره پرسنل نظامی و کار آنها جمع‌آوری کند.[۲۱۳]

۱۷ـ۲ـ Chipping

وین شوراتو در کتاب خود به نام «جنگ اطلاعات» به بحث درباره احتمال تولید ریزتراشه‌های تروایی[۱] می‌پردازد، فرآیندی که او chipping می‌نامید. این تراشه‌ها، شبیه تراشه‌های قانونی خواهند بود، اما طوری طراحی و مهندسی می‌شوند که دربرگیرنده دستورهای مخربی هم باشند. این دستورات می‌توانند باعث شوند تا تراشه پیش از موعد از کار بیفتد یا از توانایی استراق سمع پشتیبانی کند. شوارتو می‌گوید که صنایع نظامی، بازار مطلوبی برای این کار با حمایت دولت خواهد بود. هیچ گزارش مورد تأییدی از chipping مطرح نشده است.[۲۱۴]

---

1. Trojan Microchips

۱۸ـ۲ـ نرم‌افزارهای جاسوسی

تبلیغات بنری، روش رایجی برای سازندگان بسیاری از برنامه‌های نرم‌افزاری جهت کسب درآمد بیشتر، بدون پرداخت پولی برای استفاده از نرم‌افزارشان است. در عوض، فضایی هم در برنامه‌هایشان برای شرکت‌های تبلیغاتی کنار می‌گذارند. این برنامه‌های نرم‌افزاری اغلب رایگان و قابل دانلود هستند. شما هم به‌جای رایگان بودن آن، شرایط تبلیغات بنری را بر روی کامپیوترتان می‌پذیرید. این دسته از برنامه‌ها، نرم‌افزارهای حامی تبلیغاتی هستند که به صورت خلاصه "Ad ware" نامیده می‌شوند.

Ad ware، بخش معمولی زندگی امروزی اینترنت است که امکان تولید بسیاری از نرم‌افزارها را بدون اینکه در مقابل آنها پولی بپردازید، می‌دهند. اما تمام شرکت‌های تبلیغاتی در مقابل کاری که انجام می‌دهند، صادق نیستند! برنامه‌های Ad ware، آنها نه تنها تبلیغات بنری را بر روی صفحات کامپیوترتان نمایش می‌دهند، بلکه به‌طور مرموزی عادات وب گردی شما را پیگیری می‌کنند و اطلاعات جمع‌آوری شده را به شرکت‌های تبلیغاتی گزارش می‌دهند. برنامه‌های Ad ware بنرهایی را انتخاب می‌کنند که مطابق ذوق و سلیقه شماست و سپس آن بنرها را بر روی مانیتورتان ظاهر می‌سازند. به علاوه ممکن است، عادات وب‌گردیتان به شخص ثالثی هم فروخته شود!!!

این نوع از برنامه‌های تبلیغاتی به صورت برنامه‌های جاسوسی یا Spyware شناخته می‌شوند. چون در حقیقت، این شرکت‌ها از نحوه کارشان سخنی به میان نمی‌آورند و به صورت مرموزی از شما جاسوسی می‌کنند. برنامه‌های بازاریاب این شرکت‌ها در برنامه‌های معمولی‌ای که شما از اینترنت دانلود می‌کنید، مخفی شده‌اند.

نرم‌افزارهای جاسوسی[1] چگونه بر روی کامپیوتر شما قرار می‌گیرند؟

پاسخ به این سؤال بسیار ساده است. رایج‌ترین راهی که در این مورد اتفاق می‌افتد، نصب

1. Spyware

برنامه‌های رایگانی با عنوان Ad ware/ Spy ware است. Spyware، در برنامه‌ای که نصب می‌کنید، پنهان است، بنابراین نصب بودن آنها را نمی‌بینید. زمانی که Spyware بر روی کامپیوتر شما نصب شد به صورت پس‌زمینه به فعالیت می‌پردازد و شما از فعالیت آن بی‌خبر می‌مانید.

اگر فرزندانتان هم به صورت مشترک از کامپیوتر شما استفاده می‌کنند، احتمالاً دوست دارند برنامه‌های فراوانی را که بر روی اینترنت عرضه می‌شود، برای خود دانلود کنند. بعضی از این برنامه‌های رایگان ممکن است حاوی Spyware باشند و کامپیوتر شما هم ممکن است به این نوع از برنامه‌ها آلوده شود. چون فرزندانتان آنها را بدون آگاهی شما بر روی کامپیوترتان نصب کرده‌اند.

زمانی که Spyware بر روی کامپیوتر شما قرار می‌گیرد، چه کاری انجام می‌دهد؟

هدف Spyware، ارائه بازخورد بازار به شرکت یا شرکت‌هایی که آنرا در اختیار می‌گیرند، است. عادات وب‌گردی، شما را دنبال می‌کند و آنها را به صاحبش گزارش می‌دهد، بدون اینکه بدانید، چنین کاری را انجام می‌دهد. چه احساسی خواهید داشت، وقتی متوجه شوید یک شرکت بازاریاب ناشناس، تمام عادات وب‌گردیتان را بدون اجازه شما ضبط می‌کند؟ مطمئناً این نوع از پیگیری‌های استفادهٔ افراد از اینترنت، تجاوزی به زندگی خصوصی افراد است و نباید انجام بگیرد.

چه نتایج دیگری با وجود Spyware بر روی کامپیوترتان صورت خواهد گرفت؟

یکی از بیشترین مشکلات رایج شده توسط Spyware در سیستم‌تان، از کار افتادن آن است. اگر سرعت سیستم عاملتان کاهش یافته، متوقف شده و یا از کار افتاده است، شاید Spyware مخفی شده در کامپیوترتان، در حال کلنجار رفتن با سیستم عامل است.

اگر در حال حاضر بر روی کامپیوتر خود Spyware داشته باشید، چگونه آنرا می‌یابید؟

بسیاری از کاربران، Spyware را بر روی سیستم‌شان دارند، بدون اینکه آنرا شناسایی کنند. گر بخواهید آنرا شناسایی یا پاک کنید، به برنامه‌ای نیاز دارید که آنرا بر روی کامپیوترتان

تشخیص دهید و سپس آنرا شناسایی کرده و پاک کنید. برنامهٔ رایگان Ad-Aware تنها چیزی است که نیاز دارید.

برنامه Ad-Aware خود را اینگونه توصیف می‌کند؛

Ad-Aware، سیستم‌تان را برای شناسایی ترکیبات Spyware اسکن می‌کند و به شما اجازه می‌دهد تا آنها را از روی سیستم خود حذف کنید، بنابراین به صورت Online به روز می‌شود تا همیشه از شر آخرین Spy wareها رهایی می‌یابید.

به سایت http://www.lavasoftusa.com بروید و برنامه‌ای به نام Ad-Aware را دانلود کرده و بر روی کامپیوترتان نصب کنید. این برنامه بر روی هارد دیسک‌تان به جست‌وجو برای شناسایی Spyware می‌پردازد. زمانی که کار آن به پایان رسید، لیستی از Spywareهای احتمالی را به شما نمایش می‌دهد که با انتخاب هریک می‌توانید آنها را از روی کامپیوترتان بردارید.

چگونه می‌توان مطمئن شد که برنامه‌هایی را که می‌خواهیم از اینترنت دانلود کنیم، به Spyware آلوده نیست؟

یک سایت مفید برای بررسی Spyware، سایت http://www.spywarechecker.com است که به شما خواهد گفت، نرم‌افزار رایگانی را که قصد دارید از اینترنت بگیرید، حاوی Spyware است یا خیر؟ فقط نام برنامه را در قسمت جست‌وجو وارد کنید تا سایت در بانک اطلاعاتی خود دنبال برنامه مورد نظر بگردد، به عنوان مثال می‌توانید به فرزندانتان بگویید که هیچ برنامه‌ای را قبل از چک کردن توسط این سایت از اینترنت دانلود نکنند.[۲۱۵]

۱۹ـ۲ـ دفاع در برابر کرم‌ها و ویروس‌ها

کرم‌ها، نوع خاصی از برنامه‌های کامپیوتری هستند که پس از آغاز فعالیت خود، بدون مداخله انسانی منتشر و توزیع خواهند شد. ویروس‌ها، نوع دیگری از برنامه‌های کامپیوتری هستند که به منظور انتشار و توزیع خود نیازمند انجام عملیات خاصی توسط کاربر، نظیر فعال شدن فایل

همراه یک نامه الکترونیکی می‌باشند. کاربران در اغلب موارد و با مشاهده فایل‌های ضمیمه همراه نامه‌های الکترونیک[1]، اغوا شده و بدون لحاظ کردن مسائل امنیتی، آنان را بازکرده و به عاملی برای گسترش یک ویروس تبدیل می‌کنند. کاربران به دلیل کنجکاوی مربوط به موضوع یک نامه و یا ظاهر شدن نامه به گونه‌ای که برای مخاطب خود آشنا است، اقدام به باز نمودن ضمائم یک نامه الکترونیکی می‌نمایند. کرم‌ها و ویروس‌ها می‌توانند اقدامات پیشگیرانه امنیتی، نظیر فایروال‌ها و سیستم‌های حفاظتی را نادیده و اهداف خود را دنبال کنند.

کرم‌ها و ویروس‌ها در مقایسه با گذشته، با سرعت به مراتب بیشتری اقدام به خرابی سیستم‌های آسیب‌پذیر نموده و در این راستا نسخه‌هایی از خود را برای اکثر سیستم‌های فوق، توزیع و منتشر می‌نمایند. کامپیوترهای موجود در منازل، نمونه مناسبی از سیستم‌های آسیب‌پذیری بوده که شرایط و استعداد مناسبی را در این رابطه دارند.

کرم Code Red در سال ۲۰۰۱ به سرعت در سطح جهان منتشر شد. سرعت انتشار این کرم، به مراتب بیش از کرم Morris در سال ۱۹۸۸ و ویروس ملیزا در سال ۱۹۹۹ بود. بدیهی است، افزایش سرعت انتشار این نوع از کدهای مخرب، سرعت در بروز خرابی و آسیب را به دنبال خواهد داشت. مثلاً، فاصله زمانی بین شناسایی اولین نسخه کرم Code Red و خرابی گسترده آن، صرفاً چندین روز بیشتر نبوده و در این فاصله زمانی نامحدود، Code red به سرعت اشاعه و گسترش یافته است. پس از گذشت یک ماه از ظهور کرم Code red، کرم دیگری با نام «نیمدا» توانست در اولین ساعت فعالیت خود، خرابی بسیار گسترده‌ای را ایجاد نماید. در ژانویه همان سال نیز «اسلامر» صرفاً توانست در مدت چندین دقیقه، خرابی گسترده‌ای را به‌وجود آورد.

۲۰ـ۲ـ عملکرد کرم‌ها و ویروس‌ها

در بهترین حالت، کرم‌ها و ویروس‌ها به منزله مزاحمانی هستند که به‌منظور برخورد با آنان باید هزینه‌های بسیاری صرف شود و در بدترین حالت، آنان به منزلهٔ دشمنان خانمان‌سوزی هستند

---

1. Attachment

که قادرند سرمایه‌های اطلاعاتی را نابود و ویران نمایند. بر اساس گزارشات منتشر شده، صرفاً در دوازده ماه گذشته، حملات کرم‌ها و ویروس‌ها میلیون‌ها دلار خسارت را متوجه سازمان‌ها و مؤسسات کرده است.

بر اساس نظرسنجی انجام شده توسط CSI/FBI در سال ۲۰۰۳، بیش از ۸۲ درصد از پاسخ‌دهندگان با نوع خاصی از حملات توسط ویروس‌ها و کرم‌ها برخورد داشته که هزینه‌ای معادل ۲۷,۳۸۲,۳۴۰ دلار صرف برطرف نمودن مشکلات مربوطه شده است. کمترین هزینه گزارش شده، ۴۰,۰۰۰ دلار و بیشترین هزینه گزارش شده بالغ بر ۶,۰۰۰,۰۰۰ دلار بوده است. در یک نظرسنجی دیگر و در استرالیا نیز نتایجی مشابه به دست آمده است. در این نظرسنجی بیش از ۸۰ درصد از پاسخ‌دهندگان درمورد نوع خاصی از حملات توسط کرم‌ها و یا ویروس‌ها مواجه بوده‌اند. در بررسی انجام شده توسط مؤسسه تحقیقاتی استرالیا ۳۳ درصد از پاسخ‌دهندگان اعلام کرده‌اند که مشکل آنان در کمتر از یک روز، ۳۰ درصد بین یک تا هفت روز و ۳۷ درصد دیگر اعلام کرده‌اند که بیش از یک هفته صرف برطرف نمودن مشکل خود کرده‌اند. (برخی از سازمان‌ها و مؤسسات نیز اعلام کرده‌اند که مشکل آنان هرگز برطرف نشده است).

میزان صدمات و خرابی گزارش شده در ارتباط با کرم بلستر، بالغ بر ۵۲۵ میلیون دلار و در ارتباط با سوبیگ(نوع F)، بین ۵۰۰ میلیون تا یک میلیارد دلار برآورد شده است. هزینه فوق، شامل از دست دادن بهره‌وری، ساعات تلف شده، عدم فروش کالا و یا خدمات و هزینه‌های اضافی مربوط به پهنای باند است. بر اساس اظهارات ارائه شده در نشریه اکونومیست در تاریخ ۲۳ اگوست ۲۰۰۳، سوبیگ (نوع F)، مسئول یکی از شانزده نامه الکترونیکی ارسال شده بر روی اینترنت بوده است. برخی سازمان‌های بزرگ، صرفاً طی یک روز، بیش از ۱۰,۰۰۰ نامه الکترونیکی آلوده را دریافت نموده‌اند (در هر ۸/۶ ثانیه، یک پیام). سوبیگ، قادر به ارسال چندین نامه الکترونیکی در یک زمان بود و بدین ترتیب ضریب نفوذ و اشاعه آن در حد بالایی قرار داشت.(هزاران پیام در یک دقیقه). با توجه به اینکه، سوبیگ چندین‌بار تغییر و نسخه‌های

جدیدتری از آن ارائه می‌شد، برخورد و غیر فعال کردن آن با مشکل مواجه می‌شد. (حرف F نشان دهنده نسخه شماره شش سوبیگ است).

وضعیت آینده

نتایج و تجارب کسب شده، صرفاً محدود به عملکرد خاص برخی از کرم‌ها و ویروس‌ها، نظیر بلستر[1] و سوبیگ بوده و بنابراین ما باید به این واقعیت مهم توجه نمائیم که.کرم‌ها و ویروس‌ها یک تهدید جدی در رابطه با امنیت اینترنت بوده و می‌توانند مسائل متعدد و غیرقابل پیش‌بینی را در آینده برای هر یک از شهروندان حقوقی و یا حقیقی اینترنت به‌دنبال داشته باشند. بنابراین، می‌توان این ادعا را داشت که اینترنت نه تنها در حال حاضر در مقابل اینگونه حملات آسیب‌پذیر است، بلکه آسیب‌پذیری آن در آینده نیز قابل پیش‌بینی و واقعیتی غیرقابل کتمان است. کامپیوترهای موجود در سازمان‌ها، مؤسسات دولتی و خصوصی، مراکز تحقیقاتی، مدارس و دانشگاه‌ها در حال حاضر نسبت به ضعف‌های امنیتی کشف شده، آسیب‌پذیر بوده و قطعاً نسبت به ضعف‌هایی که در آینده مشخص می‌گردند، نیز آسیب‌پذیری خود را خواهند داشت. بنابراین، سیستم‌های کامپیوتری هم در مقابل حملات در حال حاضر و هم در برابر حملات در آینده، دارای استعداد لازم به منظور پذیرش آسیب خواهند بود. بدیهی است، همزمان با افزایش وابستگی سازمان‌ها و مؤسسات دولتی و خصوصی به اینترنت، انجام فعالیت‌های تجاری، تهدیدات و خطرات خاص خود را به‌دنبال خواهد داشت.

محدودیت راه‌حل‌های واکنشی

پس از گذشت نزدیک به ۱۵ سال از عمومیت یافتن اینترنت و مطالعات گسترده انجام شده

1. Blasster

به منظور کاهش خطرات، خرابی و سرعت در تشخیص و غلبه بر حملات، می‌توان این ادعا را نمود که راه‌حل‌های واکنشی به تنهایی کافی نخواهند بود. ادعای فوق، نتیجه توجه به عوامل زیر است؛

- اینترنت در حال حاضر بیش از ۱۷۱,۰۰۰,۰۰۰ کامپیوتر را به یکدیگر متصل کرده و رشد آن همچنان ادامه دارد. در حال حاضر، میلیون‌ها کامپیوتر آسیب‌پذیر در اینترنت وجود دارند که مستعد نوع خاصی از حملات، توسط مهاجمان هستند.
- تکنولوژی حملات، بسیار پیشرفته شده و مهاجمان می‌توانند با اتکا بر آخرین فناوری‌های موجود، به سادگی از نقاط ضعف موجود در سیستم‌های آسیب‌پذیر استفاده و آسیب مورد نظر خود را به آنان برسانند (حملات مبتنی بر آخرین تکنولوژی موجود)
- در حال حاضر تعداد زیادی از حملات به صورت کاملاً اتوماتیک عمل نموده و با سرعت بسیار بالایی در اینترنت، صرف‌نظر از منطقه جغرافیایی و یا محدودیت ملی، توزیع و گسترش می‌یابند.
- تکنولوژی به کار گرفته شده در حملات بسیار پیچیده و در برخی موارد تعمد پنهانی در آنان دنبال می‌شود. بنابراین، کشف و آنالیز مکانیزم‌های استفاده شده به منظور تولید پادزهر و برطرف نمودن مشکل، مستلزم صرف زمان بسیاری خواهد بود.
- کاربران اینترنت وابستگی شدیدی به اینترنت پیدا کرده و از آن به منظور انجام کارهای حیاتی خود نظیر؛ فعالیت‌های تجاری Online استفاده می‌نمایند. کوچک‌ترین وقفه در ارائه خدمات می‌تواند از دست دادن منابع اقتصادی و به مخاطره افتادن سرویس‌های حیاتی را به دنبال داشته باشد.

توجه به هر یک از موارد ذکر شده، شاهدی است بر این ادعا که ما همچنان در معرض طیف گسترده‌ای از حملات قرار داریم. حملاتی که از دست دادن منابع اقتصادی و عدم امکان عرضه سرویس‌ها را به دنبال خواهد داشت. در این راستا، باید از تمامی امکانات و

پتانسیل‌های موجود به منظور سرعت در پاسخ و برخورد با حملات استفاده کرد. بازنگری در ره‌حل‌های موجود و استفاده از رویکردهای علمی و جامع می‌تواند عاملی مؤثر در جهت برخورد مناسب با حملات باشد.

وظایف مدیران سیستم

شناسایی تهدیدات کرم‌ها و ویروس‌ها عملیات ساده و ایستایی نبوده و در این رابطه باید از رویکردهای کاملاً پویا و مبتنی بر آخرین دستاوردهای تکنولوژی استفاده شود. با کشف بیش از چهار هزار نوع نقطه آسیب‌پذیر در طی هر سال، مدیران سیستم و شبکه در وضعیت دشواری قرار دارند. آنان با چالش‌های جدی در ارتباط با تمامی سیستم‌های موجود و Patchهای مورد نظر که برای برطرف نمودن نقایص امنیتی ارائه می‌گردد، مواجه هستند.

استفاده و به‌کارگیری Patchهای ارائه شده در عین مفید بودن به منظور مقابله با مشکل امنیتی ایجاد شده، می‌توانند زمینه بروز مسائل و اثرات جانبی غیرقابل پیش‌بینی را فراهم نمایند. در این رابطه لازم است به این نکته مهم نیز اشاره شود که پس از ارائه یک Patch امنیتی، مدت زمان بسیاری طول خواهد کشید که مدیران سیستم و یا شبکه، مشکل تمامی سیستم‌های آسیب‌پذیر خود را برطرف نمایند. مدت زمان برطرف‌سازی مشکلات و اشکالات به‌وجود آمده در برخی موارد می‌تواند ماه‌ها و یا حتی سال‌ها پس از ارائه Patch پیاده‌سازی شده، به طول انجامد، به‌عنوان مثال هنوز گزارشاتی در رابطه با ویروس ملیزا که ۴ سال از فعال شدن آن گذشته است، توسط برخی سازمان‌ها و مؤسسات در سطح جهان ارائه می‌شود. ریشه‌کن نمودن یک کرم و یا ویروس شایع، با توجه به گستردگی اینترنت، عملیاتی نیست که در یک بازه زمانی محدود، بتوان موفق به انجام آن شد، بلکه می‌باید برای نیل به موفقیت فوق، زمانِ بسیاری را صرف نمود.

شاید این سؤال مطرح گردد که دلایل چنین تأخیری در ریشه‌کن نمودن یک ویروس یا کرم چیست؟ در پاسخ می‌توان به موارد متعددی، نظیر صرف زمان زیاد، پیچیدگی گسترده آنان

و عدم اختصاص اولویت مناسب برای مقابله با آنان در یک سازمان یا مؤسسه، اشاره کرد. متأسفانه، بسیاری از مدیران شناخت کامل و جامعی نسبت به تهدیدات نداشته و هرگز به مقوله امنیت با یک اولویت سطح بالا نگاه نمی‌کنند و حتی منابع لازم را به این مقوله اختصاص نمی‌دهند. علاوه بر این، سیاست‌های تجاری در برخی موارد، سازمان‌ها را به سمت انتخاب یکی از دو گزینه؛ اهداف تجاری و نیازهای امنیتی هدایت که در اکثر موارد رسیدن به اهداف تجاری را دارای اولویت و جایگاه بالاتری برای آنان می‌داند، رهنمون می‌سازد. علاوه بر تمامی مسائل فوق، می‌باید به این نکته مهم نیز اشاره کرد که تقاضا برای مدیران سیستم ورزیده و کارشناس بیش از میزان موجود بوده و همین امر همواره استفاده از متخصصان و کارشناسان امنیتی را با مشکل جدی مواجه می‌سازد (عدم توازن بین عرضه و تقاضا)

به منظور برخورد مناسب با وضعیت فوق، مدیران سیستم در یک سازمان می‌توانند با دنبال نمودن مراحل زیر، عملیات لازم جهت تسهیل در امر حفاظت سیستم‌های سازمان را انجام دهند؛

- **اتخاذ روش‌های امنیتی؛** انتخاب سیستم‌های ارزیابی امنیت اطلاعات، مدیریت سیاست‌ها و تبعیت از روش‌های امنیتی برای تمامی سازمان‌ها (بزرگ و کوچک) امری حیاتی است. سازمان‌ها و مؤسسات می‌توانند بر اساس وضعیت موجود خود، یکی از روش‌های مناسب امنیتی را انتخاب نمایند. در این راستا می‌توان از پتانسیل‌ها و تجارب بخش دولتی و یا خصوصی و همچنین از منابع متعدد اطلاع‌رسانی موجود به منظور اتخاذ سیاست‌های کلی امنیتی استفاده کرد و پس از بررسی، نسبت به تدوین و پیاده‌سازی سیاست امنیتی در سازمان مربوطه، اقدام نمود.
- **به‌هنگام نمودن دانش و اطلاعات؛** مدیران سیستم باید به منظور ارتقای سطح دانش و معلومات خود، دوره‌های آموزشی خاصی را بگذرانند. شرکت در دوره‌های آموزشی مستمر و اختصاص وقت لازم برای استفاده مفید از دوره‌های آموزشی باید در دستور کار مدیران سیستم در سازمان‌ها و مؤسسات قرار گیرد. مدیران سیستم لازم است

ضمن آشنایی با آخرین تهدیدات و حملات با ابزارهای لازم در جهت افزایش حفاظت سیستم‌ها نیز شناخت مناسبی را پیدا نمایند. ضروری است به این نکته مهم اشاره شود که امنیت، دارای ماهیتی کاملاً پویا بوده که همزمان با بروز حملات جدید و شناسایی نقاط آسیب‌پذیر جدید به صورت روزانه تغییر و ارتقا می‌یابد. بنابراین توسط دانش استاتیک و محدود نمی‌توان با مقوله‌های پویا و گسترده برخوردی مناسب و علمی داشت.

- **آموزش کاربرانی که از سیستم‌ها استفاده می‌کنند؛** مدیران سیستم باید برنامه‌های آموزشی خاصی را در رابطه با امنیت، به منظور ارتقای دانش کاربران نسبت به مسائل امنیتی، ارائه نمایند. دوره‌ها و برنامه‌های آموزشی باید کاملاً هدفمند بوده و کاربران پس از شرکت و گذراندن دوره‌های فوق، به سطح مطلوبی از توانایی به منظور تشخیص یک مسئله، انجام عملیات لازم به منظور افزایش حفاظت سیستم و برخورد مناسب در صورت مواجه با یک مشکل امنیتی دست پیدا کرده باشند. به منظور پیاده‌سازی سیاست امنیتی در یک سازمان، وجود کاربران آگاه با مسائل ایمنی اطلاعات و حفاظت از اطلاعات حساس، امری ضروری و لازم است.

وظایف ارائه‌دهندگان تکنولوژی

مدیران سیستم با دنبال نمودن پیشنهادات ارائه شده، صرفاً قادر به حل بخش‌هایی از مسئله امنیت اطلاعات می‌باشند. با توجه به جایگاه شرکت‌های ارائه دهنده تکنولوژی، حرکات و تدابیر مثبت آنان می‌تواند، تأثیر بسزایی در جهت ممانعت و گسترش کرم‌ها و ویروس‌ها را به‌دنبال داشته باشد. با اینکه برخی شرکت‌ها به سمت ارتقا و بهبود امنیت در محصولات خود حرکت کرده‌اند، اما هنوز راهی طولانی در پیش است. متأسفانه، پیاده‌کنندگان نرم‌افزار از تجارب گذشته در رابطه با نقایص امنیتی در ارائه نسخه‌های جدید نرم‌افزار خود استفاده نمی‌نمایند. بر اساس مطالعات انجام گرفته، مشاهده شده که برخی از نقاط آسیب‌پذیر در

نسخه‌های جدید تعدادی محصولات، در نسخه‌های قبلی هم وجود داشته و تلاش مناسبی در جهت بهسازی وضعیت امنیتی نسخه جدید صورت نگرفته است.

وجود برخی از نقاط آسیب‌پذیر به دلیل عدم پیکربندی ایمن سیستم‌های عامل و برنامه‌های کاربردی است. محصولات فوق، بسیار پیچیده بوده و اغلب با غیر فعال نمودن برخی از ویژگی‌های امنیتی به مشتریان عرضه می‌شوند. شرکت‌های ارائه دهنده بر این اعتقادند که همزمان با استفاده از محصول ارائه شده، کاربران می‌توانند ویژگی‌های امنیتی غیرفعال شده را در زمان لازم و به دلخواه خود فعال نمایند. بدین ترتیب تعداد زیادی از سیستم‌های متصل شده به اینترنت دارای پیکربندی مناسب در رابطه با امنیت اطلاعات نبوده و شرایط مناسبی را برای نفوذ کرم‌ها و ویروس‌ها فراهم می‌کنند.

ارائه محصولاتی که در مقابل کرم‌ها و ویروس‌ها نفوذ ناپذیر باشند، برای هر شرکت ارائه‌کننده محصولات، امری ضروری و حیاتی است. اعتقاد به این رویکرد امنیتی که «کاربر باید مراقب باشد»، در عصر حاضر پذیرفتنی نیست، چرا که سیستم‌ها بسیار پیچیده بوده و سرعت حملات نیز باورنکردنی است و در برخی موارد نیز فرصت مناسب برای برخورد با نقص امنیتی از کاربر سلب می‌گردد. تولید کنندگان محصولات می‌توانند با اتکاء و استفاده از روش‌های مهندسی نرم‌افزار، تلاش خود را در جهت تولید محصولات مقاوم در برابر حملات، دوچندان کنند. در این راستا موارد زیر پیشنهاد می‌شود؛

- **نرم‌افزار ضد ویروس[1] (مقاوم در مقابل ویروس)**: کامپیوترها و نرم‌افزارها به منظور ایمن‌شدن در مقابل تهدیدات و حملات کرم‌ها و ویروس‌ها دارای امکانات ذاتی نیستند. طراحی کامپیوترها و یا نرم‌افزارهای کامپیوتری به گونه‌ای است که امکان توزیع و انتشار ویروس‌ها و آلودگی سیستم‌ها را فراهم می‌نماید. در برخی موارد، طراحی انجام شده به گونه‌ای است که شرایط لازم برای حملات و نفوذ کرم‌ها و

1. Antivirus Software

ویروس‌ها را فراهم و استعداد فوق در بطن محصول ارائه شده وجود خواهد داشت. اجرای یک کد نامشخص و وارده از یک منبع ناشناس و گمنام نمونه‌ای از استعداد اشاره شده در بطن محصولات بوده که امکان فعال شدن یک کد اجرایی بدون محدودیت و نظارت خاصی بر روی یک ماشین، فراهم می‌شود. بدین ترتیب سیستم در مقابل حملات ویروس‌ها، آسیب‌پذیر بوده و ضروری است تولید کنندگان، سیستم‌ها و نرم‌افزارهای خود را به گونه‌ای ارائه دهند که باعث محدودیت در اجرای کدهای وارده، به‌خصوص کدهایی که از منابع تأیید نشده و ناشناخته سرچشمه می‌گیرند، شوند. در این رابطه می‌توان از روش‌های شناخته شده و مبتنی بر مهندسی نرم‌افزار متعددی استفاده کرد.

- **کاهش خطای پیاده سازی:** اکثراً نقاط آسیب‌پذیر موجود در محصولات از خطاهای موجود در مرحله پیاده‌سازی نرم‌افزار، ریشه می‌گیرد. این نوع خطاها در محصولات باقی مانده و شاید منتظرند که در زمان به‌کارگیری نرم‌افزار شناسایی گردند! تشخیص و برطرف نمودن این خطاها، صرفاً زمانی میسر می‌شود که محصول در حال استفاده و کاربری است. در موارد بسیاری، مجدداً نقایص امنیتی مشابه به صورت پیوسته در نسخه‌های جدید محصولات، مشاهده و کشف می‌گردد. مهمترین علت بروز اینگونه نقاط آسیب‌پذیر، طراحی سطح پایین و یا عدم برخورد مناسب با خطاها در زمان پیاده‌سازی است. تولیدکنندگان و ارائه‌دهندگان محصولات نرم‌افزاری باید با مطالعه و بررسی اشتباهاتِ گذشته و به‌کارگیری روش‌های مؤثر موجود در مهندسی نرم‌افزار، سعی در کاهش حفره‌ها و نقایص امنیتی در محصولات خود نمایند.
- **پیکربندی پیش فرض با امنیت بالا:** امروزه با توجه به پیچیدگی محصولات نرم‌افزاری، پیکربندی مناسب سیستم‌ها و شبکه‌ها به منظور استفاده از تدابیر امنیتی پیش‌بینی شده، امری دشوار به نظر می‌رسد. حتی در برخی موارد، افرادی‌که دارای مهارت‌های فنی قابل قبولی بوده و آموزش‌های لازم را نیز فراگرفته‌اند، به منظور استفاده و به‌کارگیری

امکانات امنیتی در یک محصول نرم‌افزاری، دارای مشکلات خاص خود هستند. اشتباهات کوچک می‌تواند سیستم‌ها را در معرض تهدید و کاربران را با حملات غیرقابل پیش‌بینی مواجه کند. تولیدکنندگان و ارائه‌دهندگان تکنولوژی می‌توانند محصولات خود را با پیکربندی پیش فرض ایمن، ارائه نمایند. در چنین مواردی، اکثر گزینه‌ها و امکانات امنیتی موجود، به صورت پیش فرض و در زمان نصب فعال خواهند بود. بدین ترتیب کاربران در آغاز استفاده از یک محصول، نیازمند تغییرات خاصی در رابطه با پیکربندی محصول نبوده و در ادامه و در صورت ضرورت، می‌توانند پیکربندی‌های پیش فرض را متناسب با خواسته خود تغییر دهند. بنابراین، کاربران با یک سطح امنیتی قابل قبول، استفاده از محصول را آغاز می‌کنند.

وظایف تصمیم‌گیرندگان

تصمیم‌گیرندگان در یک سازمان، مؤسسه و سایر بخش‌های کلان یک کشور، می‌توانند به منظور افزایش امنیت از رویکردهای متفاوتی استفاده نمایند. در این راستا موارد زیر پیشنهاد می‌گردد:

- **تقویت انگیزه‌های لازم برای ارائه محصولات با ایمنی بیشتر و کیفیت بالا**؛ به منظور ترغیب ارائه‌دهندگان جهت تولید محصولات با کیفیت و ایمنی مناسب، پیشنهاد می‌شود که تصمیم‌گیرندگان از قدرت خرید خود به منظور تقاضای نرم‌افزار با کیفیت بالا استفاده نمایند. در هنگام تهیه نرم‌افزار و عقد قرارداد مربوطه باید عبارت «کد بی‌نقص» با صراحت در متن قرارداد آورده شود. بدین ترتیب تولیدکنندگان و ارائه‌دهندگان محصولات در مواردی که نقایص خاصی، نظیر نقایص امنیتی در محصول مربوطه تشخیص و کشف می‌گردد، ملزم به رفع عیب و اشکال موجود خواهند بود. پایبندی به رویکرد فوق، انگیزه‌های مناسبی را برای تولیدکنندگان ایجاد و هر تولیدکننده‌ای که محصول بی‌نقصی را تولید و ارائه نماید، شانس موفقیت بیشتری خواهد داشت.

در این رابطه لازم است، تصمیم‌گیرندگان با مسائل متعددی همچون فرآیندهای تهیه یک محصول آشنا و به طور مستمر اطلاعات خود را ارتقا دهند تا بتوانند در زمان لازم تصمیمات منطقی و مبتنی بر دانش را برای تهیه یک محصول اتخاذ نمایند. به منظور حمایت از چنین فرآیندهایی، تهیه‌کنندگان می‌باید آموزش‌های لازم در خصوص نظارت، سیاست‌های امنیتی، اصول و مفاهیم امنیتی و معماری مربوطه را فرابگیرند. به هر حال هدف، تهیه و به‌کارگیری سیستم‌هایی است که با روح یک سازمان مطابقت و افزایش کارآیی و بهره‌وری آن‌را به دنبال داشته باشند.

- **تحقیق در رابطه با تضمین ایمن‌سازی اطلاعات:** تصمیم‌گیرندگان، همواره باید به‌دنبال راه‌حل‌های تکنیکی به منظور افزایش ضریب امنیت اطلاعات بوده و در این راستا ضروری است، تحقیقات گسترده و سازمان‌یافته‌ای را به منظور آگاهی از روش‌های کنشگرایانه و پیشگیرانه در دستور کار خود قرار دهند (استفاده از روش‌های واکنشی و انفعالی به تنهایی کفایت نخواهد کرد). بنابراین، تصمیم‌گیرندگان می‌باید از یک برنامه منسجم تحقیقاتی حمایت کنند تا به کمک آن بتوان با رویکردهای جدید در ارتباط با امنیت اطلاعات و سیستم آشنا شد. رویکردهای فوق، شامل طراحی و پیاده‌سازی استراتژی‌ها، روش‌های بازسازی اطلاعات، استراتژی‌های مربوط به مقاومت در مقابل تهاجمات، آنالیزهای مستمر و پیاده‌سازی معماری‌های امنیتی باشد. از جمله فعالیت‌هایی که در این خصوص باید موردتوجه قرار گرفته و همچنین برای آن راهکارهای مناسب ایجاد شود، عبارتند از:

- ایجاد یک چارچوب یکپارچه و یکنواخت برای آنالیز و طراحی تضمین اطلاعات؛
- ایجاد روش‌های مستحکم و مطمئن به منظور دستیابی و مدیریت خطرات برخاسته از تهدید سرمایه‌های اطلاعاتی؛
- ایجاد روش‌های ارزیابی به منظور مشخص کردن و به‌دست آوردن نسبت «هزینه ـ مزیت»، استراتژی‌های ریسک؛

- ایجاد و استفاده از تکنولوژی‌های جدید[1] به منظور مقاومت در برابر حملات، تشخیص حملات و بازیابی خرابی‌ها؛
- ایجاد روش‌های سیستماتیک و ابزارهای شبیه‌سازی برای آنالیز حملات، تصادفات و خرابی بین سیستم‌های وابسته.

• **استفاده از متخصصان فنی بیشتر؛** تصمیم‌گیرندگان، باید از مراکز امنیتی به منظور ارتقای سطح دانش عمومی امنیت حمایت کرده تا از این طریق بتوان کارآموزان و دانشجویان را جذب و با تدوین یک برنامه آموزشی هدفمند نسبت به تربیت کارشناسان ماهر امنیتی اقدام نمود. بدیهی است، استفاده از کارشناسان فوق، به منظور ایمن‌سازی سیستم‌ها و شبکه امری ضروری و اجتناب ناپذیر است. برنامه‌های آموزشی تدوین شده باید در فواصل زمانی خاصی بازنگری شوند تا بتوان افرادی را تربیت کرد که همواره پاسخگوی نیازهای امنیتی در سطح سازمان‌ها و مؤسسات بوده و به دانش روز نیز کاملاً اشراف داشته باشند.

• **ارائه آموزش و آگاهی لازم به کاربران اینترنت؛** دستیابی آسان و وجود اینترفیس‌های مناسب، باعث شده تا کاربران با هر نوع شرایط سنی، از اینترنت در تمامی سطوح زندگی استفاده نمایند. تعداد زیادی از کاربران اینترنت دارای شناخت اندکی نسبت به تکنولوژی اینترنت و یا روش‌های امنیتی لازم برای استفاده از آن، هستند. تصمیم‌گیرندگان، می‌توانند با دنبال کردن پیشنهادات زیر، سطح دانش کاربران اینترنت را افزایش دهند؛

- طراحی و پیاده‌سازی برنامه‌ها و مواد آموزشی لازم در خصوص ارتقای سطح دانش

آموزش عمومی تمامی کاربران اینترنت، آموزش و افزایش آگاهی کاربران در خصوص خصایص امنیتی، تهدیدات، فرصت‌ها و رفتار مناسب در اینترنت به

1. Modern Technology

امری ضروری و حیاتی تبدیل شده است. در این رابطه لازم است به این نکته مهم اشاره شود که بقای سیستم وابسته به امنیت سیستم‌ها در سمت دیگر بوده و حل مشکل سیستم خود به تنهایی کافی نخواهد بود و در این رابطه لازم است به تمامی کاربران در خصوص نحوه استفاده از کامپیوترهای خود با لحاظ نمودن پارامترهای ایمنی و امنیتی، آموزش‌های لازم و مستمری ارائه گردد. علاوه بر موارد فوق، ضروری است به مصرف‌کنندگان محصولات نرم‌افزاری، آموزش‌های خاصی در رابطه با نحوه تهیه و نصب نرم‌افزارهای ایمن نیز داده شود. بدین ترتیب، تولیدکنندگان محصولات نرم‌افزاری ترغیب کمتری برای ارائه محصولات خود به نقاط آسیب‌پذیر خواهند داشت.

ـ طراحی و پیاده سازی برنامه‌های آموزشی خاص در زمینه استفاده مناسب و اولیه از کامپیوتر آموزش‌های فوق، باید به همراه آموزش‌های عمومی ارائه و نحوه استفاده از کامپیوتر به درستی تبیین گردد. این نوع از آموزش‌ها را می‌توان از سطوح پائین آموزشی، آغاز کرد. کاربران نوجوان و جوان اینترنت باید نسبت به رفتارهای درست و ناشایست در زمان استفاده از کامپیوتر به‌خصوص اینترنت، به‌درستی توجیه و آموزش‌های لازم به آنان داده شود. (مشابه آموزش‌های ارائه شده به کودکان در زمینه استفاده از کتابخانه‌ها، که چه نوع رفتاری قابل قبول است و چه نوع رفتاری پذیرفتنی نیست) در این رابطه معلمان مدارس و والدین نیز باید، آموزش‌های لازم را فراگرفته تا از یک طرف قادر به رفتاری قابل قبول در زمان استفاده از کامپیوتر و شبکه‌های کامپیوتری به‌خصوص اینترنت بوده و از طرف دیگر در جایگاه خود بتوانند نظارت لازم را انجام دهند.

ابعاد متفاوت

وابستگی ما به سیستم‌های کامپیوتری به هم مرتبط به‌خصوص اینترنت، به سرعت در حال

افزایش بوده و حتی بروز اختلال اندک توسط ویروس‌ها و کرم‌ها می‌تواند پیامدهای ناگواری را به‌دنبال داشته باشد. راه‌حل‌های واکنشی استفاده شده برای مقابله با کرم‌ها و ویروس‌ها به تنهایی کفایت نخواهد کرد. افزایش قدرت و سرعت حملات باعث شده تا زیرساخت‌های اطلاعاتی در معرض تهدید و خطر قرار داشته باشند. با دنبال نمودن راه‌حل‌های موجود می‌توان سطح مناسبی از حفاظت در مقابل تهدیدات را ایجاد کرد. به منظور ارتقا و بهبود وضعیت موجود، مدیران سیستم، ارائه‌دهندگان تکنولوژی و تصمیم‌گیرندگان می‌توانند با رعایت و پیگیری برخی اصول اولیه، زمینه برخورد با کرم‌ها و ویروس‌ها را در ابعاد متفاوت فراهم نمایند.

تغییر در طراحی نرم‌افزارها، روش‌های پیاده‌سازی، افزایش تعداد مدیران سیستم آموزش دیده، بهبود سطح آگاهی کاربران، افزایش تحقیقات در رابطه با سیستم‌های ایمن و پایدار، طراحی و پیاده‌سازی دوره‌های آموزشی خاص در رابطه با کامپیوتر و امنیت شبکه، نمونه‌هایی در این زمینه بوده که می‌توانند دستاوردهای مثبتی را در ارتباط با امنیت اطلاعات برای تمامی شهروندان اینترنت به‌دنبال داشته باشد. حرکات مثبت هر یک از شهروندان اینترنت (حقوقی و یا حقیقی) در خصوص پایبندی به اصول امنیتی، تأثیری مثبت در ایمن‌سازی سرمایه‌های اطلاعاتی به‌دنبال خواهد داشت.[۲۱۶]

۲۱ ـ ۲ـ نقش عوامل انسانی در امنیت شبکه‌های کامپیوتری

یک سیستم کامپیوتری از چهار عنصر: سخت افزار، سیستم عامل، برنامه‌های کاربردی و کاربران تشکیل می‌شود. سخت افزار شامل؛ حافظه، دستگاه‌های ورودی، خروجی و پردازشگر بوده که به عنوان منابع اصلی پردازش اطلاعات، استفاده می‌گردند. برنامه‌های کاربردی[۱] شامل: کامپایلرها، سیستم‌های بانک اطلاعاتی[۲]، برنامه‌های تجاری و بازرگانی[۳]،

1. Usage Programs
2. Information Banksystems
3. Commercial and Trade Programs

بازی‌های کامپیوتری[1] و موارد متنوع دیگری بوده که روش به خدمت گرفتن سخت افزار جهت نیل به اهداف از قبل تعریف شده را مشخص می‌نمایند. کاربران شامل؛ انسان، ماشین و دیگر کامپیوترها می‌شوند.

هر یک از کاربران سعی در حل مشکلات تعریف‌شده خود از طریق به‌کارگیری نرم‌افزارهای کاربردی در محیط سخت‌افزار می‌نمایند. سیستم عامل[2]، نحوه استفاده از سخت‌افزار را در ارتباط با برنامه‌های کاربردی متفاوتی که توسط کاربران گوناگون نوشته و اجرا می‌شوند، کنترل و هدایت می‌کند. به منظور بررسی امنیت در یک سیستم کامپیوتری، باید به تشریح و تبیین جایگاه هر یک از عناصر موجود در یک سیستم کامپیوتری پرداخته شود.

در این راستا، قصد داریم به بررسی نقش عوامل انسانی در رابطه با امنیت اطلاعات پرداخته و جایگاه هر یک از مؤلفه‌های موجود را تبیین و تشریح نماییم. اگر ما بهترین سیستم سخت‌افزاری و یا سیستم عامل را به خدمت بگیریم، اما کاربران و یا عوامل انسانی درگیر در یک سیستم کامپیوتری، پارامترهای امنیتی را رعایت ننمایند، کاری از پیش نخواهیم برد. وضعیت فوق، مشابه این است که شما بهترین اتومبیل با درجه بالای امنیت را طراحی و یا تهیه کنید، اما آنرا در اختیار افرادی قرار دهید که نسبت به اصول اولیه رانندگی توجیه نباشند.(عدم رعایت اصول ایمنی)

ما باید به مقوله امنیت اطلاعات در عصر اطلاعات نه به صورت یک کالا و یا محصول بلکه به صورت یک فرآیند نگاه کرده و امنیت را در حد یک محصول خواه نرم‌افزاری و یا سخت‌افزاری تنزل ندهیم. هر یک از موارد فوق، جایگاه خاص خود را با وزن مشخص شده‌ای دارند و نباید به بهانه پرداختن به امنیت اطلاعات وزن یک پارامتر را بیش از آن چیزی که هست در نظر گرفت و پارامتر دیگری را نادیده گرفته و یا وزن غیر قابل قبولی برای آن مشخص نمائیم. به هر حال ظهور و عرضه شگفت‌انگیز تکنولوژی‌های نو در عصر حاضر،

---

1. Computer Games

2. Operation System

تهدیدات خاص خود را نیز به‌دنبال خواهد داشت. ما باید چه کار کنیم تا از تکنولوژی‌ها استفاده مفیدی داشته و در عین حال از تهدیدات مستقیم و یا غیرمستقیم آنان نیز مصون بمانیم؟ به‌طور قطع نقش عوامل انسانی که استفاده‌کنندگان مستقیم این نوع تکنولوژی‌ها هستند، بسیار محسوس و مهم است.

با گسترش اینترنت و استفاده از آن در ابعاد متفاوت، سازمان‌ها و مؤسسات با مسائل جدیدی در رابطه با امنیت اطلاعات و تهاجم به شبکه‌های کامپیوتری مواجه هستند. صرف‌نظر از موفقیت و یا عدم‌موفقیت مهاجمان و به‌رغم آخرین اصلاحات انجام شده در رابطه با تکنولوژی‌های امنیتی، عدم وجود دانش و اطلاعات لازم (سواد عمومی ایمنی) کاربران شبکه‌های کامپیوتری و استفاده‌کنندگان اطلاعات حساس در یک سازمان، همواره به عنوان مهم‌ترین تهدید امنیتی مطرح و عدم پایبندی و رعایت اصول امنیتی تدوین شده، می‌توانند زمینه ایجاد پتانسیل‌هایی شوند که توسط مهاجمان استفاده و باعث بروز مشکل در سازمان گردد. مهاجمان همواره به‌دنبال چنین فرصت‌هایی بوده تا با اتکا به آنان به اهداف خود نایل گردند. در برخی حالات، اشتباه ما زمینه موفقیت دیگران را فراهم می‌نماید. اگر سعی نمائیم بر اساس یک روش مناسب، درصد بروز اشتباهات خود را کاهش دهیم، به همان نسبت نیز شانس موفقیت مهاجمان کاهش پیدا خواهد کرد.

مدیران شبکه[1] (سیستم)، مدیران سازمان[2] و کاربران معمولی[3] همگی عوامل انسانی در یک سازمان محسوب می‌شوند که حرکت و یا حرکات اشتباه هر شخصی می‌تواند پیامدهای منفی در ارتباط با امنیت اطلاعات را به‌دنبال داشته باشد. در ادامه به بررسی اشتباهات متداولی خواهیم پرداخت که می‌توانند توسط سه گروه یاد شده انجام و زمینه بروز یک مشکل امنیتی در رابطه با اطلاعات حساس در یک سازمان را باعث شود.

---

1. Manager System
2. Manager Organization
3. Usually user's

اشتباهات متداول مدیران سیستم

مدیران سیستم به افرادی اطلاق می‌گردد که مسئولیت نگهداری و نظارت بر عملکرد صحیح و عملیاتی سیستم‌ها و شبکه موجود در یک سازمان را بر عهده دارند. در اغلب سازمان‌ها افراد فوق، مسئولیت امنیت دستگاه‌ها، ایمن‌سازی شبکه و تشخیص ضعف‌های امنیتی موجود در رابطه با اطلاعات حساس را نیز برعهده دارند. بدیهی است، واگذاری مسئولیت‌های متعدد به یک فرد، افزایش تعداد خطا و اشتباه را به‌دنبال خواهد داشت. فشار عصبی در زمان انجام کار مستمر بر روی چندین موضوع متفاوت و به صورت همزمان، به‌طور قطع احتمال بروز اشتباهات فردی را افزایش خواهد داد. در ادامه با برخی از خطاهای متداولی که ممکن است توسط مدیران سیستم انجام و سازمان مربوطه را با تهدید امنیتی مواجه سازد، آشنا خواهیم شد.

۱) عدم وجود یک سیاست امنیتی شخصی

اکثر قریب به اتفاق مدیران سیستم دارای یک سیاست امنیتی شخصی به منظور انجام فعالیت‌های مهمی نظیر؛ امنیت فیزیکی سیستم‌ها، روش‌های بهنگام‌سازی یک نرم‌افزار و روشی به منظور به‌کارگیری Patchهای جدید در زمان مربوطه نیستند. در برخی حالات، مدیران سیستم حتی نسبت به آخرین نقاط آسیب‌پذیر تشخیص داده شده نیز آگاهی بهنگام شده‌ای را نداشته و قطعاً در چنین مواردی انتظار Patch مربوطه نیز توقعی بی‌مورد است. وجود نقاط آسیب‌پذیر در شبکه می‌تواند یک سازمان را در معرض تهدیدات جدی قرار دهد. امنیت فرآیندی است که باید به صورت مستمر به آن پرداخته شود و هرگز به اتمام نمی‌رسد. در این راستا لازم است، به‌طور مستمر نسبت به آخرین حملات به همراه تکنولوژی‌های مربوطه، آگاهی لازم کسب و دانش خود را بهنگام کنیم. اکثر مدیران سیستم، کارشناسان حرفه‌ای و خبره امنیتی نیستند، در این رابطه لازم است به منظور افزایش حفاظت و ایمن‌سازی شبکه، اطلاعات و دانش مربوطه به صورت مستمر ارتقا یابد. افرادی‌که دارای گواهینامه‌های خاص امنیتی و یا دانش و اطلاعات اضافه در رابطه با امنیت اطلاعات هستند،

همواره یک قدم از افرادی‌که مهارت آنان صرفاً محدود به شبکه است، جلوتر می‌باشند. در ادامه، پیشنهاداتی به منظور بهبود وضعیت امنیتی سازمان و افزایش و ارتقای سطح معلومات مدیران سیستم، ارائه می‌گردد:

۱ـ به صورت فیزیکی محل کار و سیستم خود را ایمن سازید. زمینه استفاده از سیستم توسط افرادی‌که در محدوده کاری شما فعالیت دارند، باید کاملاً کنترل شده و تحت نظارت باشد.

۲ـ هر بار که سیستم خود را ترک می‌کنید، عملیات logout را فراموش نکنید. در این رابطه می‌توان یک زمان time out را تنظیم کرد تا در صورت فراموش نمودن عملیات logout، سیستم قادر به حفاظت خود باشد.

۳ـ خود را عضو خبرنامه‌های متفاوت امنیتی کرده تا شما را با آخرین نقاط آسیب‌پذیر آشنا نمایند. در حقیقت آنان چشم شما در این معرکه خواهند بود (استفاده مفید از تجارب دیگران)

۴ـ سعی شود به صورت مستمر از سایت‌های مرتبط با مسائل امنیتی دیدن نموده تا در زمان مناسب با پیام‌های هشداردهنده امنیتی در رابطه با نرم افزارهای خارج از رده و یا نرم افزارهای غیر اصلاح شده (unpatched) آشنا گردید.

۵ـ مطالعه آخرین مقالات مرتبط با مسائل امنیتی[1] یکی از مراحل ضروری و مهم در فرآیند خود آموزشی (فراگیری) مدیران شبکه است. بدین ترتیب این اطمینان به وجود خواهد آمد که مدیر مربوطه نسبت به آخرین اطلاعات و مسائل مربوطه امنیتی در کمیته‌های موجود، توجیه است.

۶ـ استفاده از یادداشت‌ها و مقالات در رابطه با هر نوع اطلاعات حساس، نظیر رمزهای عبور و ID هرچیزی که ممکن است زمینه‌ساز ایجاد یک پتانسیل آسیب‌پذیر و دستیابی به سیستم مطرح شود را محدود نمائید. در صورتی که از این نوع اطلاعات استفاده می‌شود، قبل

---

1. Security Affairs

از ترک محل کار، آنها را از بین ببرید. افرادی که دارای سوءنیت بوده در محدوده کاری شما هستند، می‌توانند از مزایای ضعف‌های شناخته شده استفاده کنند، بنابراین ضروری است استفاده از چنین یادداشت‌هایی محدود و یا به طور کامل حذف گردد.

۲) اتصال سیستم‌های فاقد پیکربندی مناسب به اینترنت

همزمان با گسترش نیازهای سازمان، سیستم‌ها و سرویس‌دهندگان جدیدی بر اساس یک روال معمول به اینترنت متصل می‌شوند. به‌طورقطع توسعه سیستم با هدف افزایش بهره‌وری در یک سازمان دنبال خواهد شد. اکثر این‌گونه سیستم‌ها بدون تنظیمات امنیتی خاص به اینترنت متصل شده و می‌توانند زمینه بروز آسیب و حملات اطلاعاتی توسط مهاجمان را موجب گردند (در بازه زمانی که سیستم از لحاظ امنیتی به درستی ممیزی نشده باشد، این امر مکان‌پذیر خواهد بود).

مدیران سیستم ممکن است به این موضوع استناد نمایند که سیستم جدید بوده و هنوز شخصی آنرا نمی‌شناسد و آدرس IP آن نیز شناخته شده نیست، بنابراین امکان شناسایی و حمله به آن وجود نخواهد داشت. طرز فکر فوق، یک تهدید برای هر سازمان به شمار می‌رود. افراد و یا اسکریپت‌های پویش اتوماتیک در اینترنت، به سرعت عملیات یافتن و تخریب این نوع سیستم‌های آسیب‌پذیر را دنبال می‌کنند. در این راستا، شرکت‌های خاصی نیز وجود دارند که موضوع فعالیت آنان شبکه بوده و برای تست سیستم‌های تولیدی خود به‌دنبال سیستم‌های ضعیف و آسیب‌پذیر می‌گردند. (سیستم آسیب‌پذیر ما ابزار تست دیگران خواهد شد). به هر حال ممکن است همواره افرادی به صورت مخفیانه شبکه سازمان شما را پویش کنند تا در صورت وجود یک نقطه آسیب‌پذیر، از آن برای اهداف خود استفاده نمایند. در این راستا لازم است تهدیدات و خطرات را جدی گرفته و پیگیری لازم در این خصوص انجام شود. در این رابطه موارد زیر پیشنهاد می‌شود؛

ـ قبل از اتصال فیزیکی یک کامپیوتر به شبکه، مجوز امنیتی لازم با توجه به سیاست‌های تدوین شده امنیتی برای آن صادر گردد. (بررسی سیستم و صدور مجوز اتصال)

ـ کامپیوتر موردنظر باید شامل آخرین نرم افزارهای امنیتی لازم بوده و همچنین از پیکربندی صحیح آنان اطمینان حاصل شود.

ـ در صورتی‌که لازم است بر روی سیستم مورد نظر تست‌های شبکه‌ای خاصّی صورت پذیرد، سعی گردد امکان دستیابی به سیستم فوق از طریق اینترنت در زمان تست، مسدود گردد.

ـ در سیستمی که قصد اتصال به اینترنت وجود دارد، نباید دربرگیرنده اطلاعات حساس سازمان باشد.

ـ سیستم مورد نظر را تحت عنوان برنامه‌های موسوم به InTrusion Detection System قرار داده تا نرم‌افزارهای فوق به سرعت نقاط آسیب‌پذیر و ضعف‌های امنیتی را شناسایی نمایند.

۳) اعتماد بیش از اندازه به ابزارها و برنامه‌های پویش و بررسی نقاط آسیب‌پذیر

اغلب به منظور اخذ اطلاعات در رابطه با وضعیت جاری امنیتی شبکه استفاده می‌شود. پویشگرهای تشخیص نقاط آسیب‌پذیر، اطلاعات مفیدی در ارتباط با امنیت سیستم نظیر، مجوزهای فایل، سیاست‌های رمز عبور و سایر مسائل موجود، ارائه می‌دهند. به عبارت دیگر، پویشگران نقاط آسیب‌پذیر شبکه، امکان نگرش از دید یک مهاجم را به مدیریت شبکه خواهند داد. پویشگرهای فوق، عموماً نیمی از مسائل امنیتی مرتبط را به سیستم واگذار نموده و بنابراین نمی‌توان به تمامی نتایج به دست آمده توسط آنان بسنده کرده و محور عملیات خود را براساس یافته‌های آنان قرار دهیم. در این رابطه لازم است، متناسب با نوع سیستم عامل نصب شده بر روی سیستم‌ها از پویشگران متعدد و مختص سیستم عامل مربوطه استفاده شود (اخذ نتایج مطلوب‌تر). به هر حال استفاده از این نوع نرم‌افزارها به‌طور قطع موجب شناسایی سریع نقاط آسیب‌پذیر و صرفه‌جویی زمان می‌گردد، اما نباید این تصور وجود داشته باشد که استفاده از آنان به منزله یک راه‌حل جامع امنیتی است. تأکید صرف بر نتایج به دست آمده توسط آنان، می‌تواند نتایج نامطلوب امنیتی را به‌دنبال داشته باشد. در برخی موارد، ممکن

است لازم باشد، به منظور تشخیص نقاط آسیب‌پذیر یک سیستم، عملیات دستی انجام و یا حتی اسکریپت‌های خاصی در این رابطه نوشته شود.

۴) عدم مشاهده لاگ‌ها (Logs)

مشاهده لاگ‌های سیستم، یکی از مراحل ضروری در تشخیص مستمر و یا قریب‌الوقوع تهدیدات است. لاگ‌ها، امکان شناسایی نقاط آسیب‌پذیر متداول و حملات مربوطه را فراهم می‌نمایند. بنابراین می‌توان تمامی سیستم را بررسی و آنرا در مقابل حملات مشخص شده، مجهز و ایمن نمود. در صورت بروز یک تهاجم با استفاده از لاگ‌های سیستم، تسهیلات لازم به منظور ردیابی مهاجمان فراهم می‌گردد. (البته به شرطی که آنان اصلاح نشده باشند). لاگ‌ها را به صورت ادواری بررسی و آنها را در یک مکان ایمن ذخیره نمائید.

۵) اجرای سرویس‌ها و یا اسکریپت‌های اضافه و غیرضروری

استفاده از منابع و شبکه سازمان به‌عنوان یک زمین بازی شخصی برای تست اسکریپت‌ها و سرویس‌های متفاوت، یکی دیگر از اشتباهات متداولی است که توسط اکثریت قریب به اتفاق مدیران سیستم‌ها انجام می‌شود. دارا بودن چنین اسکریپت‌ها و سرویس‌های اضافه‌ای که بر روی سیستم اجرا می‌گردند، باعث ایجاد مجموعه‌ای از پتانسیل‌ها و نقاط ورودی جدید برای یک مهاجم می‌شود (درصورتی‌که سرویس‌های اضافه و یا اسکریپت‌ها بر روی سرویس‌دهنده اصلی نصب و تست شوند، مشکلات می‌تواند مضاعف گردد). در صورت نیاز به تست اسکریپت‌ها و یا اجرای سرویس‌های اضافه، باید عملیات مورد نظر خود را از طریق یک کامپیوتر ایزوله شده[1]، انجام داد. در این راستا هرگز از کامپیوتری که به شبکه متصل است، استفاده نشود).

اشتباهات متداول مدیران سازمان‌ها

مدیران سازمان به افرادی اطلاق می‌شود که مسئولیت مدیریت، هدایت و توسعه سازمان

1. Nonconnected to Internet

را برعهده داشته و با منابع متفاوت موجود در سازمان نظیر بودجه، سروکار دارند: امروزه استفاده از اینترنت توسط سازمان‌ها و مؤسسات، مزایای متعددی را به‌دنبال دارد. واژه بسیار متداول «تجارت الکترونیکی»[1] و استراتژی تجارت الکترونیکی، از جمله مواردی است که در هر برنامه‌ریزی تجاری به آن توجه خاصی می‌شود. در صورتی که سازمان‌ها و مؤسسات دارای یک استراتژی امنیتی مشخص‌شده‌ای نباشند، اتصال به شبکه جهانی تهدیدی در ارتباط با اطلاعات حساس خواهد بود. در ادامه نیز به برخی از اشتباهات متداولی که از ناحیه مدیران سازمان بروز کرده و تأثیری منفی در ارتباط با امنیت اطلاعات در سازمان به دنبال خواهد داشت، اشاره می‌گردد:

۱) استخدام کارشناسان آموزش‌ندیده و غیرخبره

بدون تردید، کارشناسان آموزش‌دیده و خبره، یکی از منابع ارزشمند در هر سازمان محسوب می‌گردند. و همواره نیز باید از کارشناسان ورزیده در ارتباط با امنیت یک سازمان استفاده شود. فرصت سعی و خطا نیست و ممکن است در این محدوده زمانی آنچه را که یک سازمان از دست می‌دهد به مراتب بیشتر از آن چیزی باشد که می‌خواهد به دست آورد. امنیت اطلاعات از جمله مقولاتی است که برای یک سازمان دارای جایگاهی مهم می‌باشد و همواره نیز باید بهترین تصمیم در رابطه با استفاده از منابع انسانی ماهر، اتخاذ شود. استفاده از یک کارشناس غیرماهر در امور امنیت اطلاعات و شبکه در یک سازمان، خود تهدیدی امنیتی است که بر سایر تهدیدات موجود افزوده خواهد شد. (ما نمی‌توانیم مسئولیت پیاده‌سازی استراتژی در سازمان را به افرادی واگذار نمائیم که در این رابطه اطلاعات و دانش لازم را ندارند).

۲) فقدان آگاهی لازم در رابطه با تأثیر یک ضعف امنیتی بر عملکرد سازمان

بسیاری از مدیران سازمان بر این باورند که «این مسئله برای ما اتفاق نخواهد افتاد» و بر همین اساس و طرز فکر به مقوله امنیت نگاه می‌کنند. بدیهی است در صورت بروز مشکل در سازمان، امکان عکس‌العمل مناسب در مقابل خطرات و تهدیدات احتمالی وجود نخواهد داشت و این

---

1. E-Commerce

مسئله می‌تواند به دلیل عدم آشنایی با ابعاد و اثرات یک ضعف امنیتی در سازمان باشد، بنابراین لازم است به این نکته اشاره گردد که همواره مشکل برای دیگران به‌وجود نمی‌آید بلکه، ما نیز در معرض مشکلات فراوانی قرار خواهیم داشت. بنابراین لازم است همواره و به طور مستمر، مدیران سازمان نسبت به اثرات احتمالی یک ضعف امنیتی توجیه و دانش لازم در اختیار آنان قرار گیرد. در صورت بروز یک مشکل امنیتی در سازمان، مسئله به‌وجود آمده محدود به خود سازمان نشده و می‌تواند اثرات منفی متعددی در ارتباط با ادامه فعالیت سازمان به‌دنبال داشته باشد. در عصر اطلاعات و دنیای شدید رقابت، کافی است برای لحظاتی سازمانی آن چیزی باشد که نباید باشد، همین امر کافی است تا تلاش چندین ساله یک سازمان از بین برود و در برخی حالات هم حتی فرصت جبران آن نیز وجود نخواهد داشت.

تأثیر منفی بر سایر فعالیت‌های تجاری Online سازمان، عاملی برای توزیع اطلاعات غیر مفید و غیر قابل استفاده در یک چرخه تجاری، عرضه اطلاعات حساس مشتریان به یک مهاجم و به مخاطره افتادن اطلاعات خصوصی مشتریان، آسیب جدی به وجهه سازمان و به‌دنبال آن از دست دادن مشتریان و همکاران تجاری.

۳) عدم تخصیص بودجه مناسب برای پرداختن به امنیت اطلاعات

مجاب کردن یک مدیر سازمان مبنی بر اختصاص بودجه مناسب برای پرداختن به مقوله امنیت اطلاعات در سازمان از جمله مواردی است که چالش‌های خاص خود را به همراه خواهد داشت. مدیران، تمایل دارند بودجه را به حداقل مقدار خود برسانند، چرا که آنان یا اطلاعات محدودی در رابطه با تأثیر وجود ضعف‌های امنیتی در عملکرد سازمان دارند و یا در برخی حالات بودجه آنان را برای اتخاذ تصمیم مناسب محدود می‌کند. اینترنت، یک شبکه جهانی است که فرصت‌های جذاب و نامحدود تجاری را برای هر بنگاه تجاری فراهم می‌نماید و با رعایت امنیت اطلاعات و حفاظت مناسب از داده‌های حساس، امکان استفاده از فرصت‌های تجاری بیشتری برای یک سازمان فراهم خواهد شد. بنابراین، با اختصاص یک بودجه مناسب برای پرداختن و بها دادن به مقوله امنیت اطلاعات در یک سازمان،

پیشگیری‌های لازم انجام و در صورت بروز مسائل بحرانی، امکان تشخیص سریع آنها و انجام واکنش‌های مناسب فراهم می‌گردد.

به عبارت دیگر با در نظر گرفتن بودجه مناسب برای ایمن‌سازی سازمان، بستر مناسبی برای حفاظت سیستم‌ها و داده‌های حساس در یک سازمان فراهم خواهد شد. به‌طور قطع تولید و عرضه سریع اطلاعات در سازمان‌های مدرن و مبتنی بر اطلاعات، یکی از مهم‌ترین شاخص‌های رشد در عصر حاضر بوده و هر آن چیزی که می‌تواند خللی در فرآیند فوق ایجاد نماید، باعث توقف و گاهی برگشت به عقب یک سازمان، می‌گردد.

۴) اتکای کامل به ابزارها و محصولات تجاری

اگر از یک سازمان سؤال شود که چگونه خود را در مقابل حملات حفاظت نموده‌اید؟ اغلب آنان در پاسخ خواهند گفت: «ما از یک دیوار آتش[1] شناخته شده و یک برنامه ویروس‌یاب[2] بر روی سرویس‌دهنده استفاده می‌کنیم، بنابراین ما در مقابل حملات ایمن خواهیم بود». توجه داشته باشید که امنیت یک فرآیند است نه یک محصول که با خریداری آن خاطر خود را در ارتباط با امنیت آسوده نماییم.

ضروری است، مدیران سازمان شناخت مناسب و اولیه‌ای از پتانسیل‌های عمومی یک دیوار آتش و یا برنامه‌های ویروس‌یاب داشته باشند (قادر به انجام چه کاری می‌باشند و چه کاری را نمی‌توانند انجام دهند. مثلاً اگر ویروس جدیدی نوشته و در شبکه توزیع شود، برنامه‌های ویروس‌یاب موجود قادر به تشخیص و برخورد با آن نخواهند بود. این نوع برنامه‌ها صرفاً پس از مطرح شدن یک ویروس و آنالیز نحوه عملکرد آن باید به هنگام شده تا بتوانند در صورت بروز وضعیتی مشابه با آن برخورد نمایند). ابزارهایی همچون دیوار آتش و یا برنامه‌های ویروس‌یاب، بخشی از فرآیند مربوط به ایمن‌سازی اطلاعات حساس در یک سازمان بوده و با به کارگیری آنها نمی‌توان این ادعا را داشت که سازمان به‌طور کامل در مقابل تهاجمات، حفاظت خواهد شد.

---

1. Firewall
2. Virus Finder Program

۵) سرمایه‌گذاری در ارتباط با امنیت

امنیت مفهومی فراگیر و گسترده بوده که نیازمند هماهنگی و سرمایه‌گذاری در دو بعد تکنولوژی و آموزش است. هر روز ما شاهد ظهور تکنولوژی‌های جدیدی هستیم و نمی‌توانیم در مواجهه با یک تکنولوژی جدید به صورت انفعالی برخورد کرده و یا عنوان کنیم که ضرورتی به استفاده از این تکنولوژی خاص نداریم. به کارگیری تکنولوژی عملاً صرفه‌جویی در زمان و سرمایه مادی را به‌دنبال داشته و این امر باعث ارائه سرویس‌های مطلوب‌تر و ارزان‌تر به مشتریان خواهد شد. موضوع فوق هم از جنبه یک سازمان حائز اهمیت است و هم از نظر مشتریان، چرا که ارائه سرویس مطلوب با قیمت تمام شده مناسب یکی از مهم‌ترین اهداف هر بنگاه تجاری محسوب شده و مشتریان نیز همواره به‌دنبال استفاده از سرویس‌ها و خدمات با کیفیت و قیمت مناسب هستند. استفاده از تکنولوژی‌های جدید و سرویس‌های مرتبط با آن، همواره تهدیدات خاص خود را به دنبال خواهد داشت. بنابراین لازم است به این موضوع نیز توجه شود که امنیت، یک سرمایه‌گذاری پیوسته را طلب می‌نماید، چرا که با به خدمت گرفتن تکنولوژی‌های نو به منظور افزایش بهره‌وری در یک سازمان، زمینه پرداختن به امنیت باید مجدداً و در ارتباط با تکنولوژی مربوطه بررسی و در صورت لزوم، سرمایه‌گذاری لازم در ارتباط با آن صورت پذیرد. تفکر اینکه، امنیت یک نوع سرمایه‌گذاری یکبار مصرف است، می‌تواند از یک سو سازمان را در استفاده از تکنولوژی‌های نو با تردید مواجه سازد و از سویی دیگر، با توجه به نگرش مقوله امنیت (یکبار مصرف)، بهای لازم به آن داده نشده و بنابراین شروع مناسبی برای پیاده‌سازی یک سیستم امنیتی و حفاظتی مناسب را نداشته باشیم.

اشتباهات متداول کاربران معمولی

کاربران به افرادی اطلاق می‌شود که طی روز با داده‌های حساس در یک سازمان سروکار داشته و تصمیمات و فعالیت‌های آنان، داده‌های حساس و مقوله امنیت و حفاظت از اطلاعات را تحت تأثیر مستقیم قرار خواهد داد.

در ادامه با برخی از اشتباهات متداولی که این نوع استفاده‌کنندگان از سیستم و شبکه مرتکب می‌شوند، اشاره می‌گردد؛

۱) تخطی از سیاست امنیتی سازمان

سیاست امنیتی سازمان، اعلامیه‌ای است که به صورت جامع، مسئولیت هر یک از پرسنل سازمان (افرادی که به اطلاعات و سیستم‌های حساس در سازمان دستیابی دارند) در ارتباط با امنیت اطلاعات و شبکه را تعریف و مشخص می‌کند. سند و یا اعلامیه مورد نظر، به‌عنوان بخش لاینفک در هر مدل امنیتی به کار گرفته شده در سازمان محسوب می‌گردد. هدف اعلامیه فوق، ارائه روشی آسان به منظور شناخت و درک ساده نحوه حفاظت سیستم‌های سازمان در زمان استفاده است. کاربران معمولی، عموماً تمایل به تخطی از سیاست‌های تدوین شده امنیتی در یک سازمان داشته و این موضوع می‌تواند عاملی مهم برای تحت تأثیر قرار دادن سیستم‌های حساس و اطلاعات مهم سازمان در مواجهه با یک تهدید باشد. پیامد این نوع عملیات، بروز اشکال و خرابی در رابطه با اطلاعات ارزشمند در یک سازمان خواهد بود. به همین دلیل است که اکیداً توصیه می‌شود اطلاعات لازم در رابطه با نقش کاربران در تبعیت از سیاست‌های امنیتی در سازمان به آنها یادآوری و بر آن تأکید گردد.

۲) ارسال داده حساس بر روی کامپیوترهای منزل

یکی از خطرناک‌ترین روش‌ها در رابطه با داده‌های حساس موجود در یک سازمان، فعالیتی است که باعث غیرفعال شدن تمامی پیشگیری‌های امنیتی ایجادشده و درگیر شدن آنها در یک فرآیند غیرامنیتی می‌شود. پرسنل سازمان عادت دارند، اطلاعات حساس سازمان را بر روی کامپیوتر منزل خود داشته باشند تا از این طریق امکان اتمام کار خود در منزل را پیدا کنند و به این موضوع توجه نکرده‌اند که تغییر محیط ایمن سازمان با کامپیوتر منزل خود که دارای ایمنی به مراتب کمتری است، به‌طور جدی اطلاعات را در معرض آسیب و تهاجم قرار خواهد داد. در صورتی‌که ضروری است، اطلاعات را به کامپیوترهای منزل فوروارد[1] کنیم، اما

---

1. Forward

در عین حال باید یک سطح مناسب ایمنی وجود داشته باشد تا این اطمینان حاصل شود که نوت‌بوک‌ها و یا کامپیوترهای منازل در مقابل مهاجمان اطلاعاتی حفاظت شده و ایمن هستند.

۳) یادداشت داده‌های حساس و ذخیره غیرایمن آنان

ایجاد و نگهداری رمزهای عبور قدرتمند، فرآیندی مستمر است که همواره باید مورد توجه قرار گیرد. کاربران همواره از این موضوع نفرت دارند که رمز عبورهایی را ایجاد نمایند که نمی‌توانند آنها را به یاد آورند. سیاست امنیتی تدوین‌شده سازمان باید تعیین نماید که یک رمز عبور چگونه ایجاد و نگهداری شود. به خاطر سپردن چنین رمز عبوری همواره مسائل خاص خود را خواهد داشت. به منظور حل اینگونه مسائل، کاربران تمایل دارند که یادداشت‌های مخفی را نوشته و آنها را زیر صفحه کلید، کیف جیبی و یا هر مکان دیگری در محل کار خود نگهداری نمایند.

یادداشت‌های فوق، شامل اطلاعات حساس در ارتباط با داده‌های مربوط به رمز عبور و سایر موارد مرتبط است. استفاده از روش‌های فوق دارای نگهداری اطلاعات، یک تخطی امنیتی است و در این راستا ضروری است، کاربران توجیه و به آنان آگاهی لازم داده شود که با عدم رعایت موارد مشخص شده امنیتی، پتانسیل‌های لازم به منظور بروز مشکل در سیستم افزایش خواهد یافت. همچنین، لازم است به کاربران، روش‌ها و تکنیک‌های متفاوت به خاطر سپردن رمز عبور آموزش داده شود تا زمینه استفاده کاربران از یادداشت برای ثبت اینگونه اطلاعات حساس کاهش یابد، سناریوهای متفاوت برای آنان تشریح و گفته شود که یک مهاجم با استفاده از چه روش‌هایی ممکن است به اطلاعات ثبت شده در یادداشت‌ها، دست پیدا نموده و زمینه بروز مشکل را فراهم نماید.

۴) دریافت فایل از سایت‌های غیرمطمئن

یکی از سرویس‌های اینترنت، امکان دریافت فایل توسط کاربران است. کاربران به منظور دریافت فایل از اینترنت، اغلب از امتیازات خود تعدی و حتی سیاست‌های موجود در سازمان را نیز در معرض مخاطره و آسیب قرار می‌دهند. دریافت فایل از وب سایت‌های گمنام و یا

غیرمطمئن باعث کمک در توزیع برنامه‌های مهاجم در اینترنت می‌شود. بدین ترتیب ما به عنوان ابزاری برای توزیع یک برنامه مخرب در اینترنت تبدیل خواهیم شد. فایل‌ها و برنامه‌های دریافتی پس از آلودگی به نوع خاصی از برنامه مخرب (ویروس، کرم و اسب تروا)، می‌تواند تأثیرات منفی فراوانی را در ارتباط با عملکرد یک سازمان به‌دنبال داشته باشد. کاربران باید به ندرت فایل‌هایی را از اینترنت دریافت کنند و در مواردی‌که ضرورت این کار احساس و به برنامه‌ای خاص نیاز باشد، اکیداً توصیه می‌شود که موضوع با دپارتمان(IT یا سایر بخش‌های مسئول در سازمان) در میان گذاشته شود تا آنان بر اساس تجربه و دانش خود، اقدام به تهیه برنامه مورد نظر از منابع مطمئن نمایند.

۵) عدم رعایت امنیت فیزیکی

میزان آگاهی و دانش کاربران در رابطه با رعایت مسائل ایمنی به‌خصوص امنیت فیزیکی، به طرز کاملاً محسوسی افزایش امنیت و حفاظت داده‌های حساس در یک سازمان را به‌دنبال خواهد داشت. عموماً، رفتار کاربران در زمان استفاده از ایستگاه‌های کاری سازمان، سهل‌انگارانه و فاقد سواد عمومی ایمنی است. کاربران، اغلب ایستگاه‌های کاری خود را بدون در نظر گرفتن امنیت فیزیکی رها و screensaver آنان، به ندرت دارای رمز عبور بوده که این می‌تواند باعث بروز مسائل متعددی گردد. ضروری است، به کاربران آموزش‌های لازم در رابطه با استراتژی‌های متفاوت به منظور استفاده از سیستم‌های سازمان داده شود. مطمئن باشید آنها قادرند به درستی با اطلاعات حساس در سازمان برخورد نمایند و همواره پیامدهای عدم رعایت امنیت فیزیکی به آنان یادآوری می‌شود.[۲۱۷]

پی‌نوشت‌ها:

1. "The Intelligent War Signals Intelligence Demands Adaptable. Systems", International Defense Review, Jane's Information Group, Ltd., Dec 1, 1997.
2. An Appraisal of Technologies of Political Control, Report From the European Parliament Scientific and Technological Options Assessment, Jan 1998.
3. Title 18 U.S.C., Chapter 119-Wire and Electronic Communications Interception and Interception of Oral Communications.
4. "Bank to Reissue 7,700 ATM Cards", Omaha World-Herald, Feb 12, 1989; David Thompson, "Fraud Plot Allegations Stun Some", Omaha World Herald, Feb 19, 1989.
5. Sharon Walsh, "Owner of Spy Shop Chain, 2 Executives Plead Guilty", Washington Post, Mar 10, 1996.

۶. آرمن، ترسسیان، سایت Itiran

http://www.itiran.com/artic/show-user-archive.asp?des=8105&id=4

۷. همان

8. Jonathan Littman, The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen, Little, Brown and Co., 1997, pp. 121-125, 164-169.
9. This Case was brought to my attention by Hugh Blanchard.
10. Joshua Cooper Ramo, "Crime Online", Time Digital, Sep 23, 1996, pp. 28-32.
11. "1998 CSI/FBI Computer Crime and Security Survey", Computer Security Issues & Trends, Vol. IV, No. 1, Winter 1998.
12. Zachary Lum, "COMINT Goes to Hell", Jouranl of Electronic Defense, Jun 1998, http://www.jedefense.com

13. Peter G. Neumann, Computer Related Risks, ACM Press, 1995, p. 186. Attributed to San Francisco Examiner, Nov 1, 1992.
14. Barbara Kantrowitz, "The Woman We Loved", Newsweek, Sep 8, 1997, p. 46.
15. Peter G. Neumann, Computer Related Risks, ACM Press, 1995, p.186. Attibuted to San Francisco Examiner, Nov 1, 1992.
16. Jeannine Aversa, "Soldering Gun-Wielding Congressman Shows How It's Done", Associated Press, Feb 5, 1997.
17. Sharon Walsh, "3 Charged in N.Y. in Pager Scheme", Washington Post, Aug 28, 1997.
18. Dan Mitchell, "Did Breaking News Network Break the Law?" Wired News, Aug 28, 1997.
19. Dan Brekke, "Who Needs Crypto? Paging Bill Clinton", Wired News, Sep 22, 1997; Reuters, Sep 19, 1997.
20. Donald P. Delaney, Dorothy E. Denning, John Kaye, and Alan R. McDonald, "Wiretap Laws and Procedures: What Happens When the U.S. Government Taps a Line", Sep 23, 1993, http://www.cs.georgetown.edu/~denning.
21. Title 18 U.S.C., Sections 2510-2521.
22. Title 50 U.S.C., Sections 1801-1811.
23. Final Report of the Select Committee to Study Governmental Operations With respect to Intellignce Activities, United States, Washington DC, Apr 26, 1974.
24. Louis J. Freeh, Statement before the Subcommittee on Technology and the Law, Committee on the Judiciary, United States Senate, and the Subcommittee on Civil and Constiutional Rights, Committee on the Judiciary, House of Representatives, Mar 18, 1994.
25. Ibid
26. 1996 Wiretap Report, Administrative Office of the United States Courts, Washington, DC.
27. "Eavesdropping on the Rise", Intelligence Newsletter, No. 314, Jun 26, 1997.
28. Louis J. Freeh, Statement before the Subcommittee on Technology and the Law of the Committee on the Judiciary, United States Senate, and the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, House of Representatives, Mar 18, 1994, pp. 32-34.
29. CDT Policy Post, The Center for Democracy and Technology, Vol. 3, No. 15, Dec 16, 1997; Comments of the Center for Democracy and

Technology Before the FCC, CC Docket No. 97-213, May 20, 1998.
30. Statement of Louis J. Freeh, Director Federal Bureau of Investigation, before the Committee on Commerce, Science, and Transportation, United States. Senate, regarding the Impact of Encryption on Law Enforcement and Public Safety, Mar 19, 1997.
31. "Police Listened in on Bosnian Serb President, New York Times, Aug 19, 1997, p. A6.
32. "No Such Agency: America's Fortress of Spies", The Sun, reprint of a six-part Series that appeared in the Baltimore Sun", Dec 3-15, 1995.
33. Ibid
34. Ibid
35. Duncan Campbell, "Somebody's Listening", New Statesman, Aug 12, 1988; Nicky Hager, Secret Power, Craig Cotton Publishing, New Zealand, 1996.
36. Nicky Hager, Secret Power, Craig Cotton Publishing, New Zealand, 1996.
37. Ibid.
38. "Cooking up a Charter for Snooping", Connected, Issue 936, Dec 16, 1997.
39. Simon Trump, "Spy Station F83", Sunday Times, Internet Edition, May 31, 1998.
40. Guess Who Eles Was Listening to Newt Gingrch's Phone Call-and to Those of Millions of Other Americans Every Day?" Center for Security Policy, No. 97-C 9, Jan 16, 1997; "Russian Spy Network in Cuba", Associated Press, Apr 3, 1998.
41. Peter Schweizer, Friendly Spies, Atlantic Monthly Press, 1993, pp. 83-84.
42. Robert Karniol Bangkok, "Myanmar Spy Center Can Listen in to Sat-Phones, "Janes Defence Weekly, Vol. 028/011, Sept 19, 1997.
43. Frank Greve, "French Techno-Spies Bugging U.S. Industries", San Jose Mercury News, Oct 21, 1992, p. IF.
44. Peter Schweizer, Friendly Spies, Atlantic Monthly Press, 1993, pp. 122-124.
45. "An Appraisal of Technologies of Political Control", report from the European Parliament Scientific and Technological Options Assessment, Jan 1998.
46. Phil Zimmermann, "Introduction", The Zimmermann Telegram, Vol. 1.0, Spring 1997; David Kahn, The Codebreakers, Macmillan, 1967, pp. 282-297.
47. David Kahn, The Codebreakers, Macmillan, 1967, p. 297.
48. Kenneth W. Dam and Herbert S. Lin, eds., Cryptography's Role in

Securing the Information Society, National Academy Press, 1996, pp. 96-98; "No Such Agency: America's Fortress of Spies", The Sun, reprint of a six-part series that appeared in the Baltimore Sun, Dec 3-15, 1995.

49. Hugo Gurdon, "Boy, 12, Restores Reputation of US Navy Captain", International News Electronic Telegraph, Apr 27, 1998.
50. "No Such Agency: America's Fortress of Spies, "The Sun, reprint of a six-part series that appeared in the Baltimore Sun, Dec 3-15, 1995 p. 3; Kenneth W. Dam and Herbert S. Lin, eds., Cryptography's Role in Securing the Information Society, National Academy Press, 1996, pp. 95-99.
51. Roberto Suro and Peter Slevin, "Fired CIA Operative Accused of Spying", Washington Post, Apr 4, 1998.
52. Walter Pincus and Bill Miller, "Ex-CIA Operative Pleads Guilty to Blackmail Attempt at Agency", Washington Post, Jul 28, 1998.
53. Title 18 U.S.C., Chapter 26.
54. Wayne Wilson, "E-Mail Leads Police to Fugitive", Mercury Center, Aug 12, 1997.
55. Edward W. Desmond, "The Scariest Phone System", Fortune, Oct 13, 1997.
56. 1998 CSI/FBI Computer Crime and Security Survey, Computer Security Issues & Trends, Vol. IV No. 1, Winter 1998.
57. Winn Schwartau, Information Warfare, 2nd ed., Thunder's Mouth Press, 1996, p. 195, citing Toll Fraud and Telabuse: A Multibillion Dollar Problem, Telecommunications Advisors, 1992.
58. M. E. Kabay, "The InfoSe Year in Review, NCSA News, Jan 1997, p.24, citing PA News, Oct 29, 1996.
59. P. N. Grabosky and Russell G. Smith, Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities, 1997, citing D. Peachey and J. Blau, "Fraud Spreading in Corporate Nets", Communications Week Internatnal, No. 137, Jan 16, 1995, p. 1.
60. Peter Hoath, "Telecoms Fraud, the Gory Details," Computer Fraud & Security, Jan 1998, pp. 10-14.
61. Langford Anderson, "Doing Time on the Telephone Line", Security Management, Feb 1990, pp. 31-36.
62. Peter Grabosky and Russell G. Smith, Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities, 1997.
63. Langford Anderson, "Doing Time on the Telephone Line", Security Managemen , Feb 1990, pp. 31-36.

64. http://crunch.woz.org/crunch; private interview with John Draper in 1990.
65. "UK Businesses Threatened by Phone Fraud", Computer Fraud & Security,Dec 1996, p. 2.
66. Vic Sussman, "Policing Cyberspace", U.S. News & World Report, Jan 23, 1996, pp. 55-60.
67. Langford Anderson, "Doing Time on the Telephone Line", Security Management, Feb 1990, pp. 31-36.
68. Vic Sussman, "Policing Cyberspace", U.S. News & World Report, Jan 23, 1996, pp. 55-60.
69. Peter Hoath, "Telecoms Fraud, the Gory Details", Computer Fraud & Security, Jan 1998, pp. 10-14.
70. CITE Report, Tracking Number 3941997, Aug 16, 1997, at http://www.iwar.org.
71. Steven Slatem, "Hackers Break into Macedonian Foreign Ministry Phones", Risks-Forum Digest, Vol. 19, Issue 46, Nov 17, 1997, citing article by Vladimir P., Central & East European CrimiScope, http://www.ceeds.cz/cee-crimiScope/sa/content/en/cee/199711/19971115-v84.htm.
72. "Computer Hacker Made Calls at FBI Expense", Reuter, Feb 26, 1997.
73. Katie Hafner and John Markoff, Cyberpunk: Outlaws and Hackers on the Computer Frontier, Simon & Schuster, 1991, pp. 26-27.
74. William J. Cook, "Voice Mail Computer Abuse Prosecutions: United States v. Douccttc", Jan 14, 1991.
75. Randy Barrett, "Netcom Voice-Mail Gets Hacked", Interactive Week Online, June 26, 1997.
76. William J. Cook, "Voice Mail Computer Abuse Prosecutions: United States v. Doucettc", Jan 14, 1991.
77. Dara Pearlman and Don Steinberg, "What Will They Hack into Next? Press '1' to Find Out", PC/Computing, Aug 1990, pp.125-126.
78. Tom Mulhall. "Where Have All the Hackers Gone? Part 3-Motivation and Deterrence", Computers and Security, Vol. 16, 1997, pp. 291-297.
79. Bruce Sterling, The Hacker Crackdown, Bantam, 1992.
80. Bill Miller, "Ringleader Pleads Guilty in Phone Fraud", Washington Post, Oct 27, 1994.
81. Associated Press, Jan 11, 1998.
82. "Bogus Dial Tones Used in Airport Calling Card Scam", Reuters, June 19, 1998; "Airport Pay Phone Taps Used to Steal Calling Cards", New York Times, July 4, 1998.

83. Secure Computing, July 1997, p. 18.
84. "GSM Alliance Certifies False and Misleading Reports of Digital Phone Cloning", Business Wire, Apr 17, 1998.
85. Joshua Cooper Ramo, "Crime Online", Time Digital, Sept 23, 1996, pp. 28-32.
86. Ibid.
87. Mike Mills, "Cellular One Suspends a Service in N.Y. Area", Washington Post, Dec 29, 1994, p. C1.
88. Associated Press, July 2, 1996.
89. "Bill to Criminalize 'Cloning' of Cell Phones Passes Senate", Associated Press, Nov 10, 1997.
90. Michael J. Sniffen, "First Computer Wiretap Leads to Charges against Argentine Man", Associated Press, Mar 29, 1996; Bob Hohler and Hiawatha Bray, "Computer Wiretap Helps Track Hacker", Boston Globe, March 30, 1996."
91. "Argentine Computer Hacker Agrees to Waive Extradition and Plead Guilty to Felony Charges in Boston", Business Wire, Dec 5, 1997, Pamela Ferdinand, "Argentine Pleads Guilty to Hacking U.S. Networks", Washington Post, May 20, 1998.
92. Stephen C. Fehr, "Spying Eyes", Washington Post, Aug 28, 1997.
93. Ibid.
94. Ibid.
95. "How CCTV Keeps Eye on Wrong People", Intelligence Newsletter, No. 321, Oct 23, 1997.
96. Douglas Hayward, "PC-Based Surveillance Cuts Car Thefts", TechWeb, Nov 4, 1997.
97. Sylvia Moreno, "In Alexandria, Fail to Stop and Camera Goes Pop!," Washington Post, Nov 13, 1997, p. D1.
98. Stephen C. Fehr, "Spying Eyes", Washington Post, Aug 28, 1997.
99. MicroChip Video Camera with Pinhole Lens & Audio, http://www.thecodex.com/spyvideo.html.
100. Andrew Pollack, "New Technology Promises 'Camera on a Chip,'" New York Times, May 27, 1997.
101. Mimi Chakraborty, "Helmet Records Crime", The Times, Mar 8, 1998.
102. Jim Wolf, "Spy-Quality Pictures for Sale Online", Reuters, Apr 5, 1998.
103. Michael J. Martinez, "Spy in Sky Looking at You", ABCNEWS.com, June 11, 1998; http://www.terraserver.com
104. "Efforts Continue to Salvage Earth Watch Satellite", Intelligence News, Jan 26,

1998; see also EarthWatch Web site at http://www.digitalglobe.com.
105. Jim Wolf, "Colorado Spy-Quality Satellite Ready to Sell Images", Reuters, Dec 25, 1997.
106. The Times Newspapers, Interface, Dec 24, 1997.
107. Warren Ferster, "DOD Wants Say in Commercial Satellite Images", Navy Times, Jan 26, 1998.
108. John Simons, "U.S. Strays from 'Open Skies', Bans Satellite Imaging of Israel", Wall Street Journal, Jul 24, 1998.
109. Walter Pincus, "Space Imagery Overhaul Aims at Better Data and Easier Access", Washington Post, Jan 20, 1998, p. A7.
110. Wim van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" PTT Dr. Neher Laboratories, Leidschendam, The Netherlands, Apr 16, 1985.
111. Winn Schwartau, Information Warfare, 2nd ed., Thunder's Mouth Press, 1996, pp. 222-231.
112. Ibid.; Ray Kaplan and Joe Kovaa, "Talking with the Computer Underground", 1993.
113. Stuart E. Johnson and Martin C. Libicki, Dominant Battlespace Knowledge, National Defense University, Oct 1995.
114. Paul Saffo, "Sensors: The Next Wave of Innovation", Communications of the ACM, Vol. 40, No. 2, Feb 1997, pp. 93-97.
115. "An Appraisal of Technologies of Political Control", report from the European Parliament Scientific and Technological Options Assessment, Jan 1998.
116. Jim Granucci, "Urban Gunshot Location System Information", memo from Redwood City Police Department, Jan 18, 1996.
117. Neil Lewis, "U.S. to Wage High-Tech War on Drugs at Border", New York Times, Sep 17, 1997.
118. Ann Marsh, "No Place to Hide", Forbes, Sep 22, 1997.
119. Robert O'Harrow Jr., "Big Brother in Workplace Bathrooms?" Washington Post, Aug 30, 1997, p. Al.
120. "Six Chosen for Micro-UAV Technology Program", Jane's Defence Weekly, Jan 7, 1998, p. 7.
121. Dale Kuska, "Micro UAVs", Naval Postgraduate School, June 1997, in Infowar Digest, Vol. 3, No. 6, March 25, 1998.
122. "This Is One Computer Bug You've Never Heard Of", Associated Press, Jan 10, 1997.
123. "Smart Bugs: They Could Be Heroes", Wired News, Dec 29, 1997.

124. Martin C. Libicki, What Is Information Warfare? National Defense University, Aug 1995, p. 22.
125. Ross J. Anderson, "Why Cryptosystems Fail", Communications of the ACM, Vol. 37, No. 11, Nov 1994, pp. 32-40.
126. Ibid.
127. Mark Brader, "Shoulder-Surfing Automated", Risks-Forum Digest, Vol. 19, Issue 70, Apr 28, 1998, citing CTV National News and CFTO News.
128. "An Appraisal of Technologies of Political Control", report from the European Parliament Scientific and Technological Options Assessment, Jan 1998.
129. Ibid.
130. Addison-Wesley, 1998.
131. Joshua Quittner, "Hacker Homecoming", Time, Jan 23, 1995.
132. Government's Sentencing Memorandum and S.G. §5K1.1 Motion, The United States District Court for the Northern District of Georgia, Atlanta Division, U.S. V. Adam E. Grant, Franklin E. Darden, Jr., and Robert J. Riggs, prepared by Kent B. Alexander, Nov 15, 1990.
133. Philip Elmer-Dewitt, "Terror or the Internet", Time, Dec 12, 1994, pp. 44 - 45.
134. Edupage, Mar 9, 1997, citing Tampa Tribune, Mar 8, 1997; Associated Press, Mar 7, 1997; Reuter, Apr 30, 1997.
135. Elka Worner, "Hacker Pleads Guilty to Fraud", United Press International, Jun 14, 1994; Jonathan Littman, The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen, Little, Brown, 1997.
136. Martin C.libicki, "What Is Information warfar?" National Defense University, Aug 1995, pp. 28-31.
137. Bob Brewin, "Rogue Transmitter Knocks out GPS Signals", Federal Computer Week, Apr 13,1998; Charles Seife, "Where Am I?" New Scientist, Jan 10, 1998.
138. Private communication, July 7, 1998. For more information, see Carlo Kopp, "The E-Bomb-A Weapon of Electrical Mass Destruction", in Winn Schwartau, Information Warfare, 2nd ed., Thunder's Mouth Press, 1996, pp. 296-333, and http://www.cs.monash.edu.au/carlo/mpubs.html Another good source is the Joint Economic Committee Hearing on Radio Frequency Weapons and Proliferation: Potential Impact on the Economy, United States Congress, Feb 25, 1998,

http://www.house.gov/jec/hearings/02-25-8h.htm.
139. Statement of David Schriner before the Joint Economic Committee. United States Congress, Feb 25, 1998. http://www.house.gov/jec/hearings/02-25-8h.htm.
140. Winn Schwartau, "HERF Guns and EMP/T Bombs", Information Warfare, pp. 269-287.
141. Steve Macko, "The Cyber Terrorists", EmergencyNet News Service, Vol. 2, No. 156, June 4, 1996; Winn Schwartau, "Class III Information Warfare: Has It Begun?", included with the ENN issue.
142. Douglas Hayward, "Terrorist Weapon Designs Hidden on the Net", TechWire, May 9,1997.
143. Douglas Hayward, "Electronic Attacks on Banks a Myth", Tech wire, Dec 4, 1997.
144. George Smith, "EMP Gun: The Chupacabras of Infowar", July 22, 1997, http://www.soci.niu.edu/~crypt.
145. "Critical Foundations: Protecting America's Infrastructures", The Report of the President's Commission on Critical Infrastructure Protection, Oct 1997, p. 15; http://www.pccip.gov.

۱۴۶.مارتین پیتر، بخش خدمات‌رسانی B.B.C

http://www.bbc.co.uk/Persian/index.shtml

۱۴۷.ویژه‌نامه کامپیوتر و اینترنت، روزنامه ابرار اقتصادی، شماره ۱۳۸۱، ص ۱۱

http://www.abrar.ws

148. Marion Lloyd, Associated Press, San Juan, Puerto Rico, Oct 1, 1997.
149. Reuters, Jan 27, 1997.
150. Joann Muller, "Vandalism Disrupts Phones, Cable TV", Boston Globe, Nov 12, 1997, p.B3.
151. Matthew J. Littleton, "Information Age Terrorism", Master's Thesis, Naval Postgraduate School, Dec 1995, p.77, Citing Eugene Moosa, "Hundreds of Police Hunt for 300 Rail Saboteurs", Associated Press, Nov 30, 1985.
152. Ibid., p.77, Citing "Radical Guerrilla Assaults Stop JNR Train Runs", Japan Economic Newswire, Nov 29, 1985.

۱۵۳.سایت فارسی رادیو آمریکا

http://www.voanews.com, Mar 21, 2003

154. Luke Reiter and Jim Louderback, "Virus Can Overwrite BIOS, Kill Data", ZDNN, July 23, 1998.
155. Robert Lemos, "CIH Virus Claims 500 Computers at One Company, 700 at Another," ZDNN, Aug 26, 1998.
156. Adam Young and Moti Yung, "Cryptovirology: Extortion-Based Security Threats and Countermeasures", Proceedings of the 1996 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, May 6-8, 1996, pp. 129-140.
157. Eugene H. Spafford, "Computer Viruses", in Dorothy E. Denning and Peter J. Denning, eds., Internet Besieged: Countering Cyberspace Scofflaws, ACM Press, 1997.
158. Fred Cohen, "Computer Viruses", Ph.D. thesis, University of Southern California, 1985.
159. "Increases in Virus Growth", Computer Fraud & Security, Feb 1998, p. 2.
160. E-mail from Digital Hackers' Alliance, May 21, 1997, http://ahrens.callnet.com/dha.
161. Jeffrey O. Kephart, Gregory B. Sorkin, David M. Chess, and Steve R. White. "Fighting Computer Viruses", Scientific American, Nov 1997, pp. 88-93.
162. Robert Slade, Guide to Computer Viruses, Springer-Verlag, New York, 1994, pp. 59-63.
163. "NCSA 1997 Computer Virus Prevalence Survey", National Computer Security Association, 1997.
164. Jeffrey O. Kephart, Gregory B. Sorkin, David M. Chess, and Steve R. White, "Fighting Computer Viruses", Scientific American, Nov 1997, pp. 88-93.
165. Robert Slade, Guide to Computer Viruses, Springer-Verlag, New York, 1994, pp. 83-89; Peter G. Neumann, Computer Related Risks, ACM Press, 1995, p. 141.
166. "NCSA 1997 Computer Virus Prevalence Survey", National Computer Security Association, 1997.
167. Computer Virus Information Pages, Data Fellows, http://www.datafellows.com/v-desc/agent.htm.
168. Heather Harreld, "Virus Infects Communications with Mir", Federal Computer Week, Oct 20, 1997.
169. http://www.mcafee.com
170. Robert Slade, Guide to Computer Viruses, Springer-Verlag, New York,

1994, pp. 70 -76.
171. Simson L. Garfinkel, "Computer Virus Book of Records", Risks-Foruni Digest, Vol. 9, Issue 66, Feb 5, 1990, citing chart 74 from the National Center for Computer Crime Data's 1989 report, Commitment to Security.
172. Eugene H. Spafford, "Computer Viruses", in Dorothy E. Denning and Peter J. Denning, eds., Internet Besieged: Countering Cyberspace Scofflaws, ACM Press, 1997; Robert Slade, Guide to Computer Viruses, Springer-Verlag, 1994.
173. T. Bruce Tober, "Interview with the Virus Writer", TechWeb, CMPnet, Mar 13, 1998.
174. CITE Report, Tracking Number: 6911997, Oct 24, 1997; http://www.iwar.org.
175. "Third. Annual Information Week/Ernst & Young Information Security Survey", Information Week, Nov 27, 1995.
176. "Fourth Annual Information Week/Ernst & Young Information Security Survey", 1996, at http://techweb.cmp.com.
177. "Fifth annual Information Week/Ernst & Young Security Survey", 1997, at http://techweb.cmp.com.
178. "The Information Security Breaches Survey 1996", DTI, ICL, UK ITSEC, NCC.
179. "1998 CSI/FBI Computer Crime and Security Survey", Computer Security Issues & Trends, Vol. IV, No. 1, Spring 1998.
180. "NCSA 1997 Computer Virus Prevalence Survey", National Computer Security Association, 1997.
181. Ibid.
182. "Internet Hoaxes", at http://ciac.llnl.gov
183. Ibid.
184. Ibid.
185. http://ciac.llnl.gov.
186. Janet Kornblum, "Yahoo Suffers Short Hack Attack", CNET, Dec 9, 1997.
187. Ferbrache, A Pathology of Computer Viruses, Springer, London, 1992.
188. Virus Bulletin, "New RedTeam Virus Stings", ZDTV News, May 1998, http:// www.zdnet.com.
189. Peter J. Denning, ed., Computers under Attack: Intruders, Worms, and Viruses, ACM Press, 1990, contains several articles on the Morris worm; Robert Slade, Guide to Computer Viruses, Springer-Verlag, New York,

1994, pp. 76-83.

190. Commitment to Security, National Center for Computer Crime Data, 1989, chart 74. Reproduced in Risks-Forum Digest, Vol. 9, Issue 66, Feb 5, 1990.

191. John A. Rochlis and Mark W. Eichin, "With Microscope and Tweezers: The Worm from MIT's Perspective", and Eugene H. Spafford, "Crisis and Aftermath", in Peter J. Denning, ed., Computers under Attack: Intruders, Worms, and Viruses, ACM Press, Addison-Wesley, 1990.

192. Eugene H. Spafford, "Crisis and Aftermath", Communications of the ACM, Vol. 32, No. 6, June 1989, pp. 678-687, in Peter J. Denning, ed., Computers Under Attack: Intruders, Worms, and Viruses, ACM Press, Addison-Wesley, 1990, pp. 223-252.

193. Suelette Dreyfus, Underground, Mandarin, Australia, 1997.

194. Ibid.

195. Peter G. Neumann, Computer Related Risks, ACM Press, 1995, pp. 165-166.

196. William M. Carley, "In-House Hackers", Wall Street Journal, Aug 27,1992.

197. Ken Thompson, "Reflections on Trusting Trust", Communications of the ACM, Vol. 27, No. 8, Aug 1984, pp. 761-763.

198. Ann O'Hanlon, "Hacker's Breach GMU Computers, Zap Student's Work", Washington Post, Aug 8, 1997, p. B1. Peter Denning provided additional information.

199. Peter G. Neumann, Computer Related Risks, ACM Press, 1995, p. 153.

200. Robert Slade, Guide to Computer Viruses, Springer-Verlag, New York, 1994, p. 54.

201. Atlanta Journal-Constitution, Nov 16, 1995, p. F7.

202. Rajiv Chandrasekaran, "AOL Subscribers Warned of 'Trojan Horse' E-Mail", Washington Post, Jun 28, 1997, p. D1. See also http://www.ncsa.com.

203. "AOL Hacker Pleads Guilty", Reuters, Jun 29, 1998.

204. Edupage, Jan 30, 1997, citing Toronto Star, Jan 29, 1997; Marshall Jon Fisher, "moldovascam.com", Atlantic Monthly, Vol. 280, No. 3, Sep 1997, pp. 19-22.

205. John D. McClain, "Firms Settle with FTC in Phone Scam", Washington Post, Nov 5, 1997, p. C10.

206. Erica Rex, "Scott McNealy's JavaOne Keynote", Java World, Apr 3, 1997.

207. David Berlind, "Norton Utilities, Internet Explorer Combo Puts Systems in Harm's Way", ZDNet, Apr 11, 1997.
208. Drew Dean, Edward W. Felten, Dan S. Wallach, and Dirk Balfanz, "Java Security: Web Browsers and Beyond", in Dorothy E. Denning and Peter J. Denning, eds., Internet Besieged: Countering Cyberspace Scofflaws, ACM Press, 1997.
209. Nick Wingfield and Alex Lash, "JcvaScript Bug Could Be Worse", CNET, Jul 11, 1997.
210. "Microsoft Net Browser Flaw Found", Associated Press, Mar 3, 1997.
211. Erich Luening, "IE Hole Exposes Local Files", CNET, Oct 17, 1997.
212. Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach, "Web Spoofing: An Internet Con Game", Proceedings of the National Information Systems Security Conference, Oct 1997.
213. "Email Relay May Compromise OPSEC", Air Force Computer Emergency Response Team Advisory, 97-47, Oct 6, 1997.
214. Winn Schwartau, Information Warfare, 2nd ed., Thunder's Mouth Press, 1996, pp. 254-268.
215. http://www.itiran.com/artic/show_user_archive.asp?des=8110&id=14
216. http://www.itiran.com/artic/show_user_archive.asp?des=8206&id=56
217. http://www.itiran.com/artic/show_user_archive.asp?des=8203&id=42

بخش سوم

جنگ رایانه‌ای در ایران

۱ـ اینترنت در ایران

برای درک آسیب‌پذیری‌های ساختار رایانه‌ای در ایران ناگزیر از ارائه چشم‌انداز ورود اینترنت به ایران و نحوه رشد و گسترش آن هستیم. هم‌اکنون طبق اعلام رسمی وزارت ارتباطات و فناوری اطلاعات بیش از ۴/۷ میلیون نفر کاربر اینترنت در ایران وجود دارد که در مقایسه با سال ۱۳۸۱ که رقم ۱/۸ میلیون نفر بود، از رشدی بیش از ۲۰۰٪ برخوردار بوده است. اینترنت نخستین‌بار در سال ۱۳۷۱ توسط مرکز تحقیقات فیزیک نظری و ریاضیات ایران زیر نظر دکتر محمدجواد لاریجانی وارد ایران شد. تا سال‌ها، فقط چند دانشگاه ایران از طریق شبکه IPM (مرکز تحقیقات فیزیک نظری) به شبکه EARN اروپا متصل بودند، تا اینکه در سال ۱۳۷۳ اولین شرکت مستقل اینترنتی تحت عنوان ندا رایانه[1] تحت حمایت شهرداری تهران تأسیس و اولین وب سایت ایرانی را در آدرس http://www.neda.net راه‌اندازی کرد. از آن سال به بعد، اینترنت به سرعت جای خود را در محافل ایرانی باز کرد، به طوری‌که هم‌اکنون بیش از ۷ هزار سایت فارسی در اینترنت فعال است و تعداد وبلاگ‌های فارسی اعم از Persianblog و Blogger و سایر سرویس‌دهنده‌های وبلاگ از مرز ۵۰ هزار گذشته و حائز رتبه سوم وبلاگ‌های جهان شده‌اند.

1. www.neda.net

مطابق اعلام مسئولان وزارت ارتباطات و فناوری اطلاعات تا پایان برنامه پنج ساله چهارم، یعنی حداقل تا سال ۲۰۰۹ تعداد کاربران اینترنت در ایران از ۱۵ میلیون نفر فراتر خواهد رفت.

آمار رشد کاربران اینترنت در ایران در فاصله سال‌های ۱۹۹۶ تا ۲۰۰۴ بدین گونه بوده است؛

۱. سال ۱۹۹۶، ۲۰۰۰ نفر

۲. سال ۱۹۹۷، ۵۰۰۰ نفر

۳. سال ۱۹۹۸، ۲۲۰۰۰ نفر

۴. سال ۱۹۹۹، ۴۸۰۰۰ نفر

۵. سال ۲۰۰۰، ۱۳۲۰۰۰ نفر

۶. سال ۲۰۰۱، ۴۱۸۰۰۰ نفر

۷. سال ۲۰۰۲، ۱۵۰۰۰۰۰ نفر

۸. سال ۲۰۰۴، ۳۷۰۰۰۰۰ نفر

۲ـ سرقت از شبکه ATM بانک ملی ایران

اگرچه سیستم بانکداری الکترونیکی (E-Banking) در ایران هنوز گسترش پیدا نکرده است، اما برخی از بانک‌ها با راه‌اندازی سیستم‌های رایانه‌ای، اقدام به ایجاد شبکه‌های کامپیوتری خدمات مالی و بانکی برای مشتریان کرده‌اند و در این راستا شرکت‌های نرم‌افزاری با استفاده از تجهیزات سخت‌افزاری و نرم‌افزاری به کمک بانک‌ها شتافته‌اند، سیستم خودپرداز اکثر بانک‌ها و از جمله سیستم ATM بانک ملی ایران از این جمله‌اند. در پاییز ۱۳۸۲، اخبار ضد و نقیضی از سرقت در شبکه ATM در برخی سایت‌های اینترنتی فارسی و یکی دو روزنامه اقتصادی ایران منتشر شد. ابتدا مقامات بانکی به کلی، این اخبار را تکذیب می‌کردند، اما سرانجام با گذشت زمان نه تنها اخبار را تأیید کردند، بلکه در تشکر از اقدامات نیروی انتظامی

و دستگاه قضایی از یکدیگر سبقت می‌گرفتند. اما روند اطلاع‌رسانی در روزهای اول باز هم ابهام‌برانگیز و حتی متناقض بود، به طوری‌که برخی منابع از نفوذ ۴ دانشجو به کامپیوتر مرکزی شرکت خدمات انفورماتیک که حساب‌های سیبا در آن نگهداری می‌شد، خبر دادند و برخی منابع دیگر از دستگیری یک هکر اینترنتی! مبلغ اعلام شده در مورد سرقت نیز به همان میزان ضد و نقیض بود.

۳ـ اظهارات قاضی پرونده ATM

قاضی حسینی، بازپرس شعبه اول دادسرای ناحیه یک عمومی و انقلاب تهران به تشریح روند رسیدگی به پرونده سرقت رایانه‌ای از بانک ملی پرداخت و از دستگیری متهم اصلی این پرونده خبر داد.

سیدعیسی حسینی در خصوص پرونده سرقت اینترنتی از بانک ملی گفت: «حدود ۵ ماه قبل، از طرف بانک ملی گزارشی مبنی بر اینکه از طریق سیستم حساب‌های سیبا از حساب دو تن از مشترکان که موجودی بالایی هم داشته‌اند، پول برداشت شده است به ما رسید».

حسینی افزود، بررسی‌های اولیه نشان داد که این سرقت از طریق اینترنت صورت گرفته و افرادی با وارد شدن به سیستم و شناسایی حساب‌ها اقدام به برداشت پول کرده‌اند. وی گفت: «با همکاری مسئولان متوجه سرنخ اصلی شدیم و دریافتیم که پول‌های برداشت شده به حساب فرد خاصی واریز شده است. پس از دستگیری این فرد مشخص شد که وی کارشناس ارشد الکترونیک و از دانشجویان نمونه کشوری است».

بازپرس این پرونده تصریح نمود؛ وی که به‌شدت در مظان اتهام بود در اظهارات اولیه خود منکر این سرقت شد، گفت: «چندی قبل هنگامی که در اینترنت مشغول چت کردن بودم به یک آگهی برخوردم که کارت‌های خالی را به قیمت خوبی می‌خریدند به بانک رفتم و با اعلام گم شدن کارت اعتباری خود در این زمینه از رئیس بانک، اطلاعاتی کسب نمودم و سپس با قرار ملاقات، کارت اعتباری خودم را به خریداران فروختم».

وی در ادامه خاطرنشان ساخت؛ این گروه پس از گرفتن کارت برای اینکه ردپایی از خود برجای نگذارند پول‌ها را از حساب سیبا برداشت می‌کردند و به حساب فردی که کارت اعتباری را از وی خریده بودند، می‌ریختند و از طریق حساب وی، پول‌ها را برداشت می‌کردند.

در حقیقت مقصد حساب، شخص ثالثی بود تا اگر روزی مدرکی پیدا کردند ردپای شخص ثالث در میان باشد.

حسینی اظهار داشت؛ متهم اول که کارت اعتباری را فروخته بود، به‌منظور تحقیقات تکمیلی در اختیار ما قرار داشت. همچنین به بانک‌ها سفارش کردیم تا مبالغ بالایی را که از حساب‌های سیبا برداشت می‌شود تحت نظر قرار دهند. خوشبختانه بانک بر حسب سفارش ما، فردی را که خواهان برداشت مبلغ کلانی از حساب سیبا بود، تحت نظر قرار می‌دهد، اما وی فوراً فرار می‌کند، ولی مدرکی از خود بر جای می‌گذارد. خوشبختانه با پیگیری‌های انجام‌شده، توانستیم فردی را که فرار کرده بود، دستگیر کنیم. این فرد نیز اعتراف کرد که به‌صورت گروهی به کلاهبرداری اقدام می‌نموده است.

قاضی حسینی با اشاره به اینکه با کمک فرد دستگیرشده تمامی اعضای ۵ نفره این باند که همگی دانشجو بودند، دستگیر شدند، افزود؛ از میان این ۵ نفر فقط یک نفر در امر رایانه تبحر داشت و در حقیقت گرداننده اصلی این باند بود.

حسینی در مورد انگیزه گرداننده اصلی این باند گفت: این شخص در بازجویی اظهار داشت که به هیچ‌وجه انگیزه مادی نداشتم و فقط برای اینکه علم خود را به رُخ دیگران بکشم، اقدام به انجام این کار کردم، زیرا در خانه سایت اینترنتی ایجاد کرده بودم و پس از اینکه به راحتی وارد حساب‌های اینترنتی شدم وسوسه گشتم که پول هم برداشت کنم.

بازپرس شعبه اول دادسرای ناحیه یک در پاسخ به پرسشی در مورد اینکه با استناد به چه قانونی آنها را مجرم می‌دانید؟ گفت: «در مورد جرائم اینترنتی در قوه قضائیه لایحه خاصی تدوین شده است که در حال حاضر، استادان فن مشغول تدوین خاص در این زمینه هستند،

اما اکنون برای تعیین مجازات جرائم رایانه‌ای و اینترنتی، مانند همین جرم رایانه‌ای فقط به قوانین عادی استناد می‌شود.

وی اظهار داشت؛ به‌نظر اینجانب در رابطه با این جرم، سرقت معنایی وجود ندارد، زیرا ربایشی در کار نبوده، بلکه رموز بانکی مربوط به حساب بانکی شخص دیگری جعل شده و با استفاده از شگردهای خاص اموالی به سرقت رفته و در حقیقت از طریق اینترنت برداشت صورت گرفته است.

وی در بخش دیگری از سخنانش اظهار داشت؛ متهم اصلی در هنگام بازجویی به نکته مهمی اشاره کرد و گفت: وقتی برای اولین بار وارد سیستم سیبا و خودپرداز بانک‌ها شدم، مشاهده کردم که سیستم کشور در این زمینه تا چه اندازه آسیب‌پذیر است.

قاضی حسینی تصریح کرد؛ پس از این هشدار، ما وارد عمل شدیم و بررسی بیشتری را انجام دادیم تا ببینیم که واقعاً این سیستم که اموال مردم از سوی آن نگهداری می‌شود تا چه حدی آسیب‌پذیر بوده و آیا اظهارات متهم اصلی صحیح بوده یا خیر؟

در بررسی‌ها مشخص شد که برخی از مسئولان در خرید، سرویس و نگهداری این سیستم‌ها، پول‌های هنگفتی را از بیت‌المال دریافت کرده‌اند و در قبال آن، سرویسی ارائه نداده‌اند. علاوه بر این سرویس‌دهی و نگهداری سیستم امنیتی یاد شده از سوی مسئولان مربوطه بدون انجام مناقصه به یک شرکت خاص واگذار شده بود. همچنین تخلفات عدیده‌ای نیز در این زمینه انجام گرفته که با همکاری مسئولان در حال بررسی تخلفات هستیم تا برخورد قانونی لازم با آنها صورت گیرد.

گفتنی است، در این خصوص برخی از مسئولان هزینه سنگینی را به بیت‌المال تحمیل کرده‌اند و در هر نوبت کارت زدن (وارد شدن کارت به دستگاه‌های خودپرداز) ظاهراً بیش از ۳۰۰ ریال به لحاظ هزینه سرویس‌دهی دریافت می‌کنند.

قاضی حسینی تصریح کرد؛ پس از رسیدگی به پرونده مذکور، پرونده دیگری نیز در زمینه

کلاهبرداری اینترنتی از حساب کوتاه‌مدت سیبای شخصی به ما ارجاع شد که نشان می‌داد گروه دیگری نیز در این زمینه فعال هستند.

حسینی در زمینه پیشگیری از جرائم اینترنتی اظهار داشت؛ متأسفانه در زمینه خرید این سیستم به کشور ما خیانت شده و می‌توان گفت که از همان ابتدا معیوب بوده است.

کشور طراح این سیستم پس از دو ماه نصب متوجه گشت که این سیستم ایراد دارد و آنرا طرد کرد، لما متأسفانه کشور ما نسبت به خرید این سیستم اقدام نمود.

سرویس‌دهی و نگهداری این سیستم نیز ناقص است، البته پیشگیری‌های اولیه صورت گرفته و راه دسترسی اینترنتی به حساب‌ها، بسته شده است به طوری‌که برای کوتاه مدت جای نگرانی وجود ندارد.

بازپرس شعبه اول دادسرای ناحیه یک عمومی و انقلاب تهران با تأکید بر اینکه باید شخص یا شرکت ثالثی هم باشد تا نگهداری و سرویس این سیستم را بر عهده بگیرد و به‌صورت شبانه‌روزی فعال باشد، توصیه کرد؛ مردم باید در نگهداری رمزها و کارت‌های سیبا دقت کنند و به راحتی آنرا در اختیار افراد ثالث قرار ندهند. همچنین بانک‌ها امین مردم هستند و باید تمامی تلاش‌های خود را صرف نگهداری امانت مردم کنند.

وی در خاتمه خاطرنشان کرد؛ خوشبختانه مبالغ سرقت‌شده ناچیز است، اما هشدار مسئولان و به خصوص دست‌اندرکاران قضایی جدی است تا در زمینه تدوین و تصویب قانون مبارزه با جرائم اینترنتی، اجتماعی و اخلاقی تسریع کنند و بتوانیم طبق قانون با متخلفان برخورد قاطعی داشته باشیم.[۱]

بازتاب رسانه‌ای سرقت از ATM

انتشار این خبر، بازتاب‌های متفاوت و گاه متضادی در پی داشت. در این میان، آنچه که کمتر مورد توجه قرار گرفت و به عبارتی دیگر اصلاً مورد توجه قرار نگرفت، برخورد با

موضوع از زاویه دقیق علمی و ارائه اطلاعاتی مستند از چند و چون واقعیت سرقت‌های کامپیوتری مالی در سطح کشورهای گوناگون جهان است.

این بازتاب‌ها به‌گونه‌ای بود که تعدادی، وقوع چنین سرقتی را در دنیای پر رمز و راز تجارت الکترونیک، عادی و رقم آنرا در مقایسه با وقوع سرقت از بانک‌ها به شیوه سنتی، ناچیز و در مقایسه با کل داد و ستد پول در شبکه بانک ملی ایران بسیار ناچیزتر قلمداد می‌کردند و گروهی دیگر نیز این سرقت را بهانه‌ای برای انتقاد از ضعف تدابیر ایمنی در شبکه بانکداری الکترونیک کشور، قرار دادند.

نوشتار زیر با استفاده از منابع به روز و دست اول بین‌المللی کوشش می‌کند تا اطلاعاتی مستند پیرامون موضوع ارائه دهد.

تلاش در دو بعد فنی و حقوقی

در مجموع، سرقت‌های مالی کامپیوتری[1] انواع گوناگونی دارند و به شیوه‌های متفاوتی هم صورت می‌گیرد، ضمن آنکه با پیشرفت تکنولوژی، روز به روز هم بر پیچیدگی و هم بر تنوع آنها افزوده می‌شود.

به همین دلیل در کشورهای صنعتی، تلاش بسیار زیادی در حال انجام است تا از یک سو، تدابیر سخت‌افزاری و نرم‌افزاری ایمنی بیشتری برای مقابله با این نوع سرقت‌ها اتخاذ شود و از سوی دیگر قوانین و مقررات جدیدتری در راستای برخورد با سارقان کامپیوتری به میان آید.

عدم وجود ایمنی صد درصد تحت هر شرایطی در هر کجای دنیا

با این همه و به‌رغم تمامی این تمهیدات، همهٔ متخصصان این رشته تردیدی ندارند که هرگز نمی‌توان شبکه‌های مالی کامپیوتری در بانک‌ها و دیگر مؤسساتی که با پول سروکار

---

1. Finance Computer Thiefs

دارند را در هیچ کجای دنیا و تحت هر شرایطی، صد درصد ایمن دانست.

مصداق این نکته، گزارش یک مرجع بین‌المللی است که صریحاً ذکر می‌کند که؛ نفوذ به داخل شبکه‌های مالی کامپیوتری که با سیستم‌هایی نظیر «مایکروسافت»[1]، «سان»[2]، «آی بی ام»[3] و «اوراکل»[4] اداره می‌شوند، کاملاً امکان‌پذیر است.

ماه‌ها برای کشف و سال‌ها برای رفع مشکل

یک بررسی انجام‌شده در آمریکا که در ماه آوریل ۲۰۰۳ (اردیبهشت ۱۳۸۲) توسط شرکتی به نام «STAR SYSTEMS» صورت گرفت، نشان می‌دهد که ۱۲ میلیون نفر از جمعیت آمریکا تنها قربانی یک‌گونه از سرقت‌های مالی کامپیوتری به نام «سرقت هویت» بوده‌اند.

گزارش شرکت «STAR SYSTEMS» بر روی این نکته تأکید می‌ورزد که آمار فوق چندان هم دقیق نیست، زیرا بخشی از این جرائم ماه‌ها ناشناخته می‌ماند، ضمن آنکه تازه زمانی‌که وقوع این سرقت‌ها کشف می‌شود، سال‌ها به طول می‌انجامد تا بتوان مشکل را حل کرد!

در همین زمینه، گزارش می‌شود که کمیسیون فدرال آمریکا در سال ۲۰۰۲، ۱۶۱۸۱۹ مورد شکایت مربوط به سرقت هویت را ثبت کرد که ۱۷ درصد آن به تقلب در امور بانکی مربوط می‌شده است.

خسارت ۲۴ میلیارد دلاری در آمریکا و قوانین جدید

موضوع فوق که طبق یک آمار، خسارتی نزدیک به ۲۴ میلیارد دلار در سال وارد می‌کند، سبب شده تا از سال ۱۹۹۸ به بعد قوانین جدیدی در این زمینه در آمریکا مطرح شود که از جمله آنها قانون «PATRIOT» می‌باشد که از مهرماه گذشته به مورد اجرا در آمده است.

---

1. Microsoft
2. Sun
3. IBM
4. Oracel

همچنین قانون دیگری به نام «BASELII» در رابطه با ریسک عملیاتی بانک‌ها مطرح است که از سال ۲۰۰۶ باید اجرا شود.

۴۰ پلیس متخصص در انگلستان و ۲۰ نفر در برزیل

موضوع جرائم اینترنتی و سرقت از بانک‌ها از طریق شبکه‌های کامپیوتری آنقدر جدید است که در کشوری مانند انگلستان، تنها ۴۰ پلیس متخصص این رشته در سال ۲۰۰۱ آموزش دیده‌اند و در حال حاضر هم فقط در لندن مستقر هستند. بنابراین، قرار است به این تعداد تا سال ۲۰۰۴، ۴۰ نفر دیگر اضافه و در سطح شهرهای دیگر انگلستان عملیاتی شوند. پلیس انگلستان تا سال ۲۰۰۴، ۲۵ میلیون پوند برای مقابله با این نوع جرائم هزینه خواهد کرد.

در کشور برزیل نیز تنها ۲۰ افسر در دایره جرائم اینترنتی فعالیت می‌کنند و در حال حاضر در «سائوپولو» پایتخت اقتصادی آن کشور، استقرار پیدا کرده‌اند. این در حالی است که در برزیل ماهانه ۲۰ مجرم اینترنتی دستگیر می‌شوند.

سه نوع اخلالگر[1]

بهتر است بر روی این نکته تأکید شود که در مجموع سه نوع اخلالگر به داخل شبکه‌های مالی کامپیوتری نفوذ می‌کنند؛

- افرادی که برای تفریح این کار را می‌کنند.
- مجرمانی که با قصد ارتکاب جرم و سرقت به این کار روی می‌آورند.
- فعالان سیاسی که در راه نیل به اهداف خود، در این زمینه گام برمی‌دارند.

هدف، شرکت‌های متصدی پردازش صورتحساب‌ها نه خود بانک‌ها

در مورد شیوه اعمال سرقت‌های اینترنتی از بانک‌ها گفتنی است که ساده‌ترین روش آن،

1. Deranger

طریقی نیست که به‌طور مستقیم خود بانک هدف قرار گیرد، بلکه کافی است تا هدف، یکی از شرکت‌هایی باشد که از سوی بانک‌ها، متصدی پردازش صورتحساب‌ها و اطلاعات می‌شوند، چه در بسیاری اوقات، بانک‌ها این اجازه را به این قبیل شرکت‌ها می‌دهند تا کل شبکه‌ها را اداره کنند.

تشکیل تیمی متشکل از شخصی از درون، یک گام ضروری

شرایط فوق در حالی است که در اغلب اوقات، تشکیل تیمی متشکل از شخصی از درون سازمان، یک گام ضروری برای نفوذ به داخل شبکه‌های مالی کامپیوتری به‌شمار می‌رود.

یک تحلیلگر وزارت خزانه‌داری آمریکا در این زمینه عقیده دارد، بیش از ۶۰ درصد نفوذهای گزارش شده به داخل شبکه‌های مالی کامپیوتری، دربرگیرنده همکاری یک فرد یا افرادی از درون بوده است.

زمان متفاوت برای سرقت مبالغ متفاوت

به عقیده کارشناسان امور ایمنی شبکه‌های مالی کامپیوتری، سرقت ۵,۰۰۰ تا ۱۰,۰۰۰ دلار از طریق نفوذ به داخل شبکه‌های کامپیوتری ظرف چند هفته صورت می‌گیرد، اما سرقت مبالغ یک میلیون دلار به چهار تا شش ماه وقت نیاز دارد.

آمارهای مربوط به سرقت‌های اینترنتی

در مورد حوادث مربوط به اینگونه سرقت‌های اینترنتی از بانک‌ها و مؤسسات مالی در کشورهای گوناگون جهان آمارهای گوناگونی ارائه شده است.

به‌عنوان مثال، یک کارشناس نفوذگری (HACK) از شرکت "PREDICTIVE SYSTEMS" که وی، متخصص مقابله و بهینه‌سازی در برابر نفوذ است، اظهارنظر می‌کند که در ماه حدود دو بار، از این شرکت برای انجام کار دعوت به‌عمل می‌آید. همچنین گزارش

شده که در سال ۲۰۰۰ بیش از ۲۰ بانک استرالیا، مورد حمله نفوذگران قرار گرفته است.

طبق گزارشی که در ماه مه ۲۰۰۳ انتشار یافت، بیش از $\frac{۱}{۳}$ بانک‌ها و شرکت‌های ارائه‌کننده خدمات مالی در سال ۲۰۰۲، موردی از نفوذ به داخل شبکه‌های کامپیوتری خود را داشتند.

شرکتی به نام "DELOITTE TOUCHE TOHAMATSUDTT" که گزارش فوق را تهیه کرده، می‌گوید؛ از ۳۹ درصد مجموع شرکت‌های خدمات مالی یا بانک‌هایی که وقوع چنین حوادثی را پذیرفتند، ۱۶ درصد آنها با حملات بیرونی، ۱۰ درصد نفوذ داخلی و ۱۳ درصد با هر دو عامل مرتبط بوده‌اند.

آسیب دیدن همزمان ۳۰۰ بانک در آمریکا

در این میان، یکی از قابل توجه‌ترین حملات نفوذی به شبکه‌های کامپیوتری بانک‌ها و مؤسسات مالی در سال ۲۰۰۲ روی داد. در این حادثه، یک شرکت ارائه‌دهنده خدمات به صنایع مالی در آمریکا به نام "S1 CORP" مورد حمله قرار گرفت و این امر باعث شد تا بیش از ۳۰۰ بانک، اتحادیه اعتباری، بیمه و شرکت‌های سرمایه‌گذاری به‌طور همزمان تحت تأثیر قرار گرفته و به‌گونه‌ای آسیب ببینند.

بانک مشهور "BARCLAYS"در انگلستان نیز در سپتامبر ۲۰۰۳، قربانی حملات نفوذی شد، ضمن آنکه در همان زمان به دو بانک کانادایی به نام "BMO" و "MOUVEMENT DES CAISSE DES JARDINS" در مونترال نیز حمله شد.

حکایت جنگجویان چچن!

در میان حملات نفوذی اینترنتی به بانک‌ها دو مورد متفاوت و جالب نیز وجود دارد. یکی از این موارد آنگونه که روزنامه ایزوستیا، چاپ مسکو در سپتامبر ۲۰۰۲ گزارش می‌کند، به سال قبل از آن یعنی ۲۰۰۱ بازمی‌گردد. در آن زمان جنگجویان چچن چندین بار تلاش نمودند تا به ۱۰ بانک بزرگ اروپایی حمله نفوذی انجام دهند.

براساس نوشته «ایزوستیا»، شیوه نفوذ در این زمینه منحصر به فرد بود و حکایت از توانمندی علمی بالای نفوذگران داشت.

YIHAT برای نفوذ به حساب‌های اسامه بن‌لادن!

مورد دیگر به تشکیل گروهی موسوم به "YIHAT" به سرپرستی یک بازرگان آلمانی در سال ۲۰۰۲ مربوط می‌شود که نوعی جنگ اینترنتی ضدترور به راه انداختند.

این گروه متشکل از ۳۴ نفر در ۱۰ کشور جهان به بانک‌هایی نفوذ کردند که تصور می‌شد اسامه بن‌لادن و گروه القاعده در آنجا حساب بانکی دارند. در مورد این گزارش، "FBI" حاضر نشد به اظهارنظر بپردازد.

علاوه بر آنچه که گفته شد، بهتر است به موارد جالب دیگری در مورد نفوذ به سیستم‌های کامپیوتری نیز اشاره شود؛

پنتاگون سالی ۱۵ میلیون حمله به خود را ثبت می‌کند!

یک آمار انتشاریافته حکایت از آن دارد که در نیمه اول سال ۲۰۰۲، بیش از ۴۰۰۰۰۰ حمله نفوذی تنها در یک بخش و آن هم در آمریکا صورت گرفته است. گفته می‌شود وزارت دفاع آمریکا (پنتاگون) به تنهایی ۱/۵ میلیون حمله نفوذی به سیستم‌های خود در سال را به ثبت می‌رساند.

کشور برزیل را «ابرآزمایشگاه جرائم اینترنتی در دنیا» به حساب می‌آورند. در این کشور ماهنامه‌ای به نام "H4CK3R" درباره دنیای زیرزمینی دیجیتال منتشر می‌شود که ۲۰۰۰۰ نسخه از آن، از طریق دکه‌های روزنامه‌فروشی به فروش می‌رسد.

از سال ۲۰۰۳ تاکنون، ۹۶۰۰۰ حمله اینترنتی در این کشور گزارش شده که در مقایسه با شمار حملات صورت‌گرفته در کشور ترکیه، شش برابر افزایش یافته است.

چنانچه نفوذگری در دادگاه آمریکا محکوم شود تا ۵ سال زندان در انتظار وی خواهد بود.

بیشترین هزینه بانک‌ها، هزینه‌های مرمت و تقویت سیستم‌ها

در مورد حملات نفوذی کامپیوتری به شبکه‌های بانکی، به این نکته مهم باید توجه داشت که بیشترین خسارت بانک‌ها در این ارتباط، فقدان پول سرقت شده نیست، بلکه هزینه‌هایی است که باید صرف مرمت و تقویت سیستم‌ها شود تا از تکرار این قبیل حملات، جلوگیری به‌عمل آید. رقمی که در این زمینه برآورد می‌شود در هر حمله نفوذی تا یک میلیون دلار برای مرمت، تقویت سیستم‌ها و مشاوره هزینه برمی‌دارد.

سالی ۱۱ میلیارد دلار خسارت مصرف‌کنندگان آمریکایی

علاوه بر این، تخمین زده می‌شود که جرائم اینترنتی در آمریکا تنها ۱۱ میلیارد دلار در سال برای شرکت‌ها و مصرف‌کنندگان هزینه برمی‌دارد که سهم رو به رشدی از این رقم، به بانک‌ها و مؤسسات مالی تعلق دارد.

براساس گزارشی که اداره پلیس فدرال آمریکا (FBI) و گروهی به نام "COMPUTER SECURITY INSTITUTE" در ماه آوریل ۲۰۰۲ انتشار دادند، به ۲۲۳ شرکت از ۵۰۳ شرکتی که به پرسش‌نامه‌های آنها پاسخ دادند، تا میزان ۴۵۵ میلیون دلار بابت سرقت‌های اینترنتی خسارت وارد آمد.

تحقیقات شرکت دیگری به نام "GARTNER" در سال ۲۰۰۲ نشان می‌دهد که ارائه‌دهندگان خدمات مالی در جهان، ۳۸۱ میلیارد دلار هزینه برای بهینه‌سازی تکنولوژی مربوط به فعالیت خود اختصاص داده‌اند که از این رقم ۱۶۳ میلیارد دلار سهم آمریکا، ۱۲۷ میلیارد دلار سهم اروپای غربی و ۵۴ میلیارد ریال هم سهم ژاپن بود.

این هزینه‌ها در حالی است که بسیاری از بانک‌ها و مؤسسات مالی به‌رغم رکود حاکم بر اقتصاد جهان درصدد برآمده‌اند تا ظرف دو سال آینده، پست جدیدی به نام «ریاست بخش امنیت سیستم‌ها» یا «امنیت اطلاعات» را درون دستگاه‌های متبوع خود به‌وجود آورند. اما، این اقدام باعث می‌شود تا مجدداً هزینه‌ها افزایش یابد.

عدم گزارش ۸۰ درصد جرائم اینترنتی به نیروی انتظامی

ناگفته نماند اعداد و ارقام فوق در حالی گزارش می‌شود که طبق گزارش بانک جهانی، ۸۰ درصد جرائم اینترنتی در بخش مالی به نیروی انتظامی گزارش نمی‌شود، ضمن آنکه کارکنان بخش تکنولوژی اطلاعات در بسیاری از بانک‌ها و مؤسسات مالی، وقوع بسیاری از این حوادث را از ترس اخراج و یا از دست دادن شغل، به اطلاع مقامات ارشد خود، نمی‌رسانند.

عدم تمایل بانک‌ها به ارائه اطلاعات

نه بانک‌ها و نه دستگاه‌هایی که مسئول نظارت بر آنها هستند، به‌ندرت حاضر می‌شوند تا اطلاعاتی مربوط به نفوذ به سیستم‌های خود را علنی کنند. در این زمینه، "John Carlson" مشاور ارشد امور تکنولوژی بانکداری در «اداره ذی‌حسابی پول» وابسته به وزارت خزانه‌داری آمریکا به صراحت، اظهارنظر می‌کند که ما واقعاً تمایلی نداریم تا این‌گونه اطلاعات را علنی کنیم؛ زیرا اگر چنین اطلاعاتی علنی شوند، در آن صورت بانک‌ها به نوبه خود از گزارش چنین مواردی خودداری خواهند کرد.

وی اضافه می‌کند؛ «اصولاً علنی کردن چنین اطلاعاتی، نوعی قضاوت زودهنگام درباره موضوع را سبب خواهد شد و این قضاوت در مورد افرادی صادق است که هیچ‌گونه اتهام رسمی علیه آنها اقامه نشده است».

نتیجه‌گیری

باید توجه داشت، شیوه‌های گوناگون حملات اینترنتی به بانک‌ها، یکی از جرائم معمول در دنیای مجازی محسوب می‌شود. جرائمی از این قبیل، برای کشورهایی که تجارت و بانکداری الکترونیک[1] در آنها پیاده‌سازی شده، به‌نوعی عمومیت یافته است. هر چند میزان نسبتاً بالای آمار مربوط به این نوع جرائم، نوعی بی‌اطمینانی نسبت به خرید و فروش "ON-LINE" را باعث می‌شود، اما اولاً؛ دایره این جرائم نسبت به جرائم بانکی و مالی که در دنیای واقعی روی

می‌دهد، به مراتب کمتر است و ثانیاً؛ تبادلات مالی در آن به مراتب ایمن‌تر صورت می‌گیـرد. از طرف دیگر، استفاده از خدمات الکترونیکی در بسیاری از کشورهای دنیا، امروزه تجربه شـده و به جهت مزیت‌ها و بهره‌وری‌های آن بـه سـرعت در سـطح جهـان در حـال گـسترش اسـت. مصداق این امر پـیش‌بینـی شـرکت "FINANCIAL INSITE" ناشـر خبرنامـه "ON-LINE "BANKING REPORT" است که بر طبق آن، شمار خانوارهای استفاده‌کننـده از بانکـداری Online از ۲۲ میلیون در سال ۲۰۰۲ بـه ۳۴ میلیـون در سـال ۲۰۰۵ افـزایش پیـدا خواهـد کرد.(۲)

۴ـ هک و نفوذ رایانه‌ای در ایران

در حالیکه بسیاری از وزارتخانـه‌هـا و سـازمان‌هـای دولتـی ایـران در حـال انجـام آزمـایش و تجربه‌های نخستین خود برای ورود بـه دنیـای اینترنـت هـستند، بـر روی جهـان پهنـاور وب موضوع امنیت برای بسیاری از سایت‌هایی که توسط افراد حقیقی و بدون کمک دولتـی ایجـاد شده‌اند، موضوعی جدی و تعیین‌کننده است. هر چند اینترنت در آغاز ورود به ایران بـا بخـش دولتی تماس برقرار کرد (مرکز فیزیک نظری ایران ـ تحت ریاست دکتر محمدجواد لاریجانی) اما ویژگی آزادمنشی و قدرت رهاکنندگی اینترنت به‌سرعت آنرا از پشت درهای بسته دولتی به میان بخش‌های خصوصی و مردم آورد. این ناهماهنگی و ناهمگونی رشـد اینترنـت در ایـران، به‌طور طبیعی آثار منفی را نیز با خود به همراه داشته است. در این میان مقوله امنیـت از همـان ابتدای ورود اینترنت به ایران موردتوجه قرار داشت، امـا بـه‌دلیـل همـه‌گیـر نـشدن و نداشـتن جایگاهی واقعی، به این موضوع توجهی جدی نشان داده نشد، اما امروزه کـامپیوتر بـه شـکلی بارز، جایگاه خود را در زندگی ایرانیان باز کرده است. اینترنت نیز اندک زمانی است که از قیـد و بند نمایش و پُز درآمده و کاربردهای آن کم‌کم در حال آشکار شدن است. در چنین شرایطی و در حالیکه آمار کاربران اینترنت ایرانی روز به روز در حال افزایش است و ایـن میـزان نـه از آمارگیری‌ها بلکه از فـروش خـوب حـساب‌هـای اینترنتـی، کـارت‌هـای اینترنتـی و همچنین

کامپیوترهای شخصی مشخص است. اخیراً نیز موضوع امنیت به همین دلیل مورد توجه بخش‌های خصوصی فعال بر روی اینترنت قرار گرفته که طی چند ماهه اخیر میزان حملات بر سایت‌های اینترنتی ایرانی رو به افزایش گذاشته و به‌خصوص بازار خدمات‌دهندگان فضا را تحت تأثیر خود قرار داده است.

هک شدن‌های متوالی و حملات هشدار دهنده متعدد در برخی اوقات بسیاری از سایت‌ها را مجبور به تغییر سرور یا جست‌وجو برای سرورهای بهتر کرده است. در چنین شرایطی موضوع امنیت، بار دیگر به بحث اصلی میان کارشناسان و کاربران این حوزه مبدل شده است و حتی بسیاری را به این فکر واداشته که اگر برای کارهای معمولی خصوصی، اطلاعات بر روی اینترنت به سادگی مورد دستبرد قرار گرفته و یا امکان ارائه آن مختل شود آن هم درست در زمانی‌که قرار است اطلاعات دولتی از طریق چنین شبکه‌ها و سایت‌هایی در اختیار همگان قرار گیرد، وضعیت چگونه خواهد بود؟ مثلاً اگر فرض کنیم اطلاعات پزشکی افراد بالاخره زمانی دیجیتالی شده و برای استفاده سریع‌تر و بهتر روی وب قرار گیرد، امکان دسترسی غیرقانونی و احتمالاً خرابکاری در این سیستم تا چه حد ممکن است ضرر و زیان‌های مادی به بار آورده و مهم‌تر از آن عملاً بی‌اعتمادی عمومی نسبت به سیستم‌های جدید خدمات‌دهی را به همراه داشته باشد.

از این‌رو امنیت، سخن اول را در ارتباطات شبکه‌ها می‌زند و این برای کشوری مانند ایران که در حال رشدی نامتوازن در عرصه فناوری اطلاعات است یک زنگ خطر محسوب می‌شود.

در تمامی برنامه‌های کلانی که در زمینه اینترنت و شبکه‌ها طرح‌ریزی می‌شود موضوع امنیت، هسته و نقطه کلیدی این‌گونه برنامه‌ها است، بدین ترتیب که بدون برقراری یک محیط امن برای ارتباط و تبادل داده‌ها و اطلاعات، امکان گسترش و تثبیت سیستم وجود ندارد. گسترش فناوری کامپیوتری در ایران همراه با مشکلات و نواقصی بوده است، به‌عنوان مثال بسیاری از نرم‌افزارهایی که در شبکه‌های داخلی مورد استفاده قرار می‌گیرند از طریق واسطه‌ها،

دلالان بازار و عموماً به‌صورت قاچاق وارد کشور می‌شوند. این‌گونه نرم‌افزارها که با قیمتی ده‌ها برابر پایین‌تر از قیمت اصلی به فروش می‌رسند، از پشتیبانی لازم شرکت‌های سازنده آن برخوردار نیستند و بالطبع آن هم از امنیت پایینی برخوردارند. استفاده از چنین مجموعه نرم‌افزارهایی برای مقاصد حرفه‌ای، مشکلات بزرگ امنیتی ایجاد می‌کند، خصوصاً در آینده که امور ایران به سمت دیجیتالی و مکانیزه شدن پیش می‌رود، امنیت نکته کلیدی و مهمی محسوب می‌شود، به‌عنوان نمونه در بحث تجارت الکترونیک تأمین امنیت قرارداد طرفین مهم‌ترین نکته به‌حساب می‌آید، بدین ترتیب که اگر در میانه قرارداد، هرگونه خدشه‌ای بدون اطلاع دو طرف در متن قرارداد صورت بگیرد، شاید باعث شود تا یکی از طرفین قرارداد به نحو غیرقابل باوری دچار ضرر و زیان شود.

حملات متعدد به سایت‌های ایرانی این پرسش را به‌وجود آورده است که در صورت گسترش فناوری‌های کامپیوتری در ایران، امنیت اطلاعات مختلف در برابر یک حمله کامپیوتری چگونه خواهد بود؟ میزان حملات اینترنتی در ایران، در مقایسه با سایر کشورهای جهان اگرچه چندان بالا نیست، اما با توجه به رشد اینترنت در کشور طی سال‌های اخیر و توجه بیشتر مردم به سایت‌های داخلی این حملات از بازتاب گسترده‌تری برخوردار شده است. در مورد سرویس‌های اینترنت، مانند Hosting به‌دلیل نداشتن زیرساخت‌های ارتباطی مانند فیبرنوری و از طرفی نبودن ارتباطی تجاری میان شرکت‌های ایرانی و طرف‌های خارجی موجب شده تا با یک بحران مواجه باشیم. تلاش برخی از خدمات‌دهندگان Hosting در داخل ایران برای رقابت و پایین آوردن غیرقابل باور قیمت‌ها برای در دست گرفتن بازار موجب شده تا کمتر به مقوله امنیت سایت‌ها توجه شود، به این ترتیب که تلاش این افراد برای جلب و جذب سایت‌های بیشتر بر روی یک سرور اصلی متمرکز بوده و بنابراین گاهی آنها بر روی یک سرور بیش از ۳۰۰ سایت را قرار می‌دادند، این کار به‌طور طبیعی امنیت سرور و سایت‌ها را پایین می‌آورد. نمونه آنرا طی ماه‌های تابستان ۱۳۸۲ شاهد بودیم که بیشترین ضرر متوجه خود مسئولان سرور و سپس مسئولان سایت‌ها بوده است.[۳]

۵ـ حمله به ۳۵۰ دامین اینترنتی ایرانی

در بزرگ‌ترین حمله اینترنتی به سایت‌های ایرانی، ۳۵۰ Domain سایت ایرانی مورد هک قرار گرفت. اواخر تیرماه ۱۳۸۲ پنل مدیریتی ثبت Domain شرکت میزبان نت Mizban.net توسط هکر ناشناسی هک شد و name Serverهای تمامی دامین‌های ثبت‌شده توسط این شرکت به‌وسیله این هکر ناشناس تعویض گشت و بیش از ۳۰۰ سایت ایرانی از جمله سایت سازمان بورس اوراق بهادار دچار اختلال شد. این مسئله تمام صاحبان سایت‌ها را دچار سردرگمی کرد، اما تمام این ماجرا به اینجا ختم نشد، بلکه فرد مذکور سایت‌های اصلی تمامی فروشندگان عمده‌ای را که با میزبان همکاری می‌نمودند، شناسایی کرده و صفحه اصلی سایت این شرکت‌ها را نیز تغییر داده و تمامی این افراد را به‌عنوان شرکت‌های کلاهبردار معرفی و لیست نمود.

از نوع عملکرد این فرد، این‌گونه به‌نظر می‌رسید که گویی تمامی شرکت‌ها را به خوبی می‌شناخته و به احتمال زیاد به‌نوعی با آنها در ارتباط بوده و با قصد و تعمد این کار را صورت داده است. میزان ضرر و زیان‌های مادی که این افراد در چنین ماجرایی متحمل شدند از دید افراد حرفه‌ای و دست‌اندرکار این حرفه پوشیده نیست. آنچه در این میان اتفاق افتاد و غیرقابل جبران است، صدمه و لطمه‌ای بود که به آبروی حرفه‌ای این افراد و شرکت‌ها وارد شد. سایت itiran در این زمینه نوشت؛ «در این ماجرا همه مقصرند، اما تقصیر اصلی بر عهده دولت است. تا زمانی‌که قوانین برخورد با متخلفان و مزاحمان اینترنتی در ایران مدون و ضامن اجرایی قوی پیدا نکند، سرمایه‌گذاری در این زمینه از امنیت بالایی برخوردار نیست و این رشته نه تنها نمی‌تواند نظر سرمایه‌گذاران عمده را به خود جلب کند، بلکه همین مقدار سرمایه‌گذار خصوصی هم به‌زودی سرمایه خود را جمع کرده و عطای سرمایه‌گذاری در این رشته را به لقائش خواهند بخشید».[۴]

۶ـ مرد عنکبوتی در ایران

رباینده ۳۵۰ دامین ایرانی خود را مرد عنکبوتی معرفی کرد. اقدام او اعتراضات فراوانی را

برانگیخت، از جمله مدیر تالار وب ایران، محمدعلی شمس‌الدین talarveb.com ضمن محکوم کردن این حرکت مرد عنکبوتی که ۳۵۰ دامین سایت‌های ایرانی را ربوده است، اعلام کرد؛ اظهارات مرد عنکبوتی جز کذب مطلق چیزی نیست و شاهد ما بر چنین مدعایی، این نکته است که تمامی سایت‌های هاست شده توسط تالار وب بر روی سرور جداگانه‌ای می‌باشد که هیچ‌گونه ارتباطی به شرکت Mizban.net و یا این بهانه که سرورهای mizban دچار ضعف امنیتی هستند، ندارد. تنها Domainهای مربوط به این شرکت (تالار وب) توسط شرکت میزبان ثبت گردیده و تحت پنل مدیریتی این شرکت بوده که توسط این هکر دزدیده و DNSهای آن تغییر داده شده است. بنابراین با تغییراتی که در دامین‌های تالار وب توسط فرد ربایند ایجاد شده، مشخص است که هدف این فرد، تنها ضربه‌زدن به آبروی شرکت‌ها و افراد متخصص دست‌اندرکار این رشته بوده است و این حرکت به جز از بین بردن سرمایه‌های ملی کشورمان و ضربه زدن به تعدادی سرمایه‌گذار خصوصی که بدون هیچ‌گونه حمایتی زندگی خود را در راه رشد IT در ایران خرج نموده‌اند و به امید بهبود این راه در ایران تلاش می‌کنند، نتیجه‌ای ندارد.

و از سویی دیگر تمامی شرکت‌ها و افرادی که در این زمینه در ایران در حال کوشش هستند، ادعایی نکرده‌اند که به‌صورت ۱۰۰ درصد توانایی برقراری امنیت سرورها را دارند، اما تا آنجایی که در حد توانمان باشد، امنیت سرورها و داده‌های مشتری را برقرار می‌سازیم و در صورتی که ادعای مرد عنکبوتی صحت داشت، شیوه درست آن بود که این ضعف امنیتی را به مسئولان میزبان اطلاع می‌داد تا آنان با کمال میل در جهت رفع ایراد تلاش نمایند، نه اینکه در این حد گسترده و غیرقابل‌جبران اقدام به ایجاد خسارت کند. در نهایت از طرف تالار وب و کلیه خسارت‌دیدگان آرزو می‌کنم که دیگر شاهد چنین حوادث کودکانه‌ای در سطح حرفه‌ای IT ایران نباشیم.

البته این مدیر شرکت اینترنتی توضیح نداد که آیا هک کردن دامین ۳۵۰ شرکت متخصص در امور کامپیوتر، شبکه و اینترنت چگونه می‌تواند «اقدامی کودکانه» باشد؟ ضمناً اعتراف ایشان به آسیب‌پذیر بودن سرورهای ایرانی برخلاف تبلیغات ایشان در رسانه‌ها است.(۵)

دستکاری در سرورItiran و ماهنامه Ccwmagazine

سایت Itiran که یکی از سایت‌های خبری مربوط به فناوری اطلاعات در ایران است، تاکنون چندین بار از سوی هکرها، دستکاری شده است، از جمله در تاریخ ۴ آذر ۱۳۸۲، مدیر این سایت اعلام کرد، به‌دلیل حمله اینترنتی به سرور آن، به مدت چند ساعت در دسترس نبود.

در این حمله اینترنتی به جز صفحه سایت IT ایران، صفحات نخست تعدادی از سایت‌هایی که روی این سرور قرار داشتند، نیز تغییر کرده و فعالیت آنها مختل شد. روز بعد از آن، شرکت میزبان، نت فایل‌های پشتیبان روز قبل را فعال کرد و بدین ترتیب ادامه فعالیت این سایت امکان‌پذیر شد.

سایت ماهنامه دنیای کامپیوتر و ارتباطات Ccwmagazine نیز که برگزارکننده مسابقه وبلاگ‌های برگزیده فارسی در اینترنت است در آذرماه سال ۱۳۸۱ درست همزمان با برگزاری مراسم اهدای جوایز برندگان، مورد هک قرار گرفت و علاوه بر آن سایت‌ها و وبلاگ‌های چند تن از برگزیدگان دستکاری شده و تصاویر مستهجنی در صفحه اول آنها قرار گرفت.[۶]

۷ـ مش قاسم، هکر ایرانی

یکی از جنجالی‌ترین موارد هک کردن وب سایت‌ها در ایران مربوط به دی‌ماه ۱۳۸۱ می‌شود که طی آن سرورها فراهاست یا در واقع در بخش وب شرکت فرارایانه نفوذ شد. تمام محتوای سایت‌های این سرور تغییر کرد و امکان بازیابی اطلاعات هم به آسانی در اختیار فراهاست نبود. رمز عبور Admin هم عوض شده و بنابراین تمام امیدها به سوی شرکت آمریکایی یا کانادایی ارائه خدمات بود. شرکت موردنظر نیز در تعطیلات آخر هفته و کریسمس به سر می‌برد و به راحتی پاسخگو نبود. هک‌کننده که خود را مش قاسم معرفی کرده بود، هدف خود را نشان دادن ایمن نبودن سرورهای ایران اعلام کرد.

تلفن‌های شرکت فرارایانه مرتب زنگ می‌خورد، صاحبان سایت‌ها ناراضی بودند و تمام تقصیرها را بر عهده شرکت یاد شده می‌انداختند که چرا سرورهایتان امن نیست یا چرا از

مشاور امنیتی استفاده نمی‌کنید؟ اما کسی توجه نمی‌کند که اتفاقاً فراهاست تا آنجا کـه امکـانش بوده هم سرورهای امنی دارد و هم از مشاوران امنیتی استفاده می‌کند، اما به چند دلیل همه چیز در اختیار خودشان نیست؛

۱. بخش وب شرکت فرارایانه ماهانه چندین میلیون تومان هزینه نگهـداری سـرورهایش را در یک کشور خارجی پرداخت می‌کند.

۲. فراهاست باید در ازای خرید نرم‌افزارهایی که ما در مجموع آن را با دو سه هزار تومـان تهیه می‌کنیم، بهای هر یک را به چند صد هزار تومان پرداخت کند.

۳. به ازای هر اشکال کوچـک در سـرورها، آن اشـکالاتی کـه امکـان رفعـش از راه دور و توسط متخصصان خودمان امکان‌پذیر نیست، فراهاست باید هزینه متخصصان مایکروسـافت را به دلار پرداخت کند تا اشکال رفع شود.

۴. با تمام شرایط فوق، باید بتواند با رقبای ایرانی‌اش رقابت کند، او باید به تومـان دریافـت کرده و به دلار هزینه کند.

۵. زمانی که مشکلی پیش می‌آید، دست هاست ایرانـی بـه جـایی نمـی‌رسـد. از آنجـا کـه سرورها باید در کشورهای اروپا، کانادا یا آمریکا باشند و تنها راه دسترسی به آنها، ایمیل، تلفـن و فاکس است، اگر کسی جواب تلفنش را نداد یا اگر پاسخ ایمیل‌هایش را نگرفت، هیچ کـاری از دستش ساخته نیست.

۶. هاست (Host) ایرانی حق انتخابی هم ندارد، سرویس بهتر، هزینـه‌هـای بـسیار بـالاتری دارد و در چنین شرایطی امکان رقابت در بازار ایران وجود نخواهد داشت.

۷. او حق انتخاب ندارد، زیرا تمام شرکت‌ها حاضر نیستند بـا ایـران همکـاری کننـد، ایـن موضوع به‌خصوص در شرایط فعلی، حقیقتی انکارناپذیر است.

۸ . فراهاست در کشوری خدماتش را عرضه می‌کند که بهترین شـرایط را دارد تـا در کنـار چین و روسیه به‌عنوان یکی از بزرگ‌ترین پرورشگاه‌های هکرها در جهان شـناخته شـود. هـیچ قانونی برای مقابله با هکرها وجود ندارد و هرکس می‌تواند این اجازه را به خودش بدهـد کـه

برای تمرین درس کلاس شبکه‌اش تمام تلاشش را برای دستکاری هرکدام از سرورهای مورد علاقه‌اش انجام دهد. این شرایطی است که گریبانگیر یک هاست ایرانی است.

وقتی سایتی هک می‌شود دو گروه متضرر می‌گردند؛ صاحبان سایت و ارائه‌دهندگان خدمات هاستینگ.[۷]

۸ـ آموزش هک در ایران!

یکی از شگفت‌آورترین پدیده‌های مرتبط با IT و اینترنت در ایران، آموزش هک به صورت علنی است.

«آموزش Hack توسط نرم‌افزار قدرتمند (Sub 7) کاملاً فارسی و مولتی مدیا صورت می‌گیرد، این نرم‌افزار برای آگاهی شما از روش‌های متداول نفوذ به رایانه‌ها در شبکه‌های داخلی و اینترنت فراهم شده است».

اینها تیترهای ریز و درشتی هستند که پشت و روی بسته‌های حاوی برنامه‌ها به چشم می‌خورند، بسته‌هایی با طراحی‌های مشخص و رنگ‌آمیزی‌هایی برای جلب توجه مشتریان خاص. چنین نرم‌افزارهایی در اکثر مغازه‌های CD فروشی در ایران یافت می‌شوند. قیمت این نرم‌افزارها، بین ۲ تا ۵ هزار تومان است که برخی شامل کتابچه راهنما یا حتی راهنمای Online هستند. بسیاری از وبلاگ‌های کامپیوتری نیز راه‌های مختلف هک کردن را به جوانان آموزش می‌دهند. مخاطبان این برنامه‌ها به‌طور عمده جوان و زیر ۲۲ سال سن دارند، این سن اوج ماجراجویی کامپیوتری است.

فروش این برنامه‌ها در تهران بنا بر گفته صاحبان فروشگاه‌های CD بسیار خوب است، نوع بسته‌بندی‌ها و قیمت‌های CDهای هک کردن و کرک کردن Crack نیز به‌گونه‌ای است که نشان می‌دهد تولیدکنندگان این برنامه‌ها، مشتریان خود را به خوبی می‌شناسند. برخی از عناوین داخلی برنامه‌های نرم‌افزاری هک کردن در ایران عبارتند از؛ ۱۲ فصل آموزش نفوذ به رایانه‌های شخصی و سیستم‌ها، نفوذ از طریق ویروس‌ها و روش‌های استفاده از آنها، پیدا کردن

کلمه‌های عبور، رمزنگاری، کرم‌های رایانه‌ای و آموزش گام به گام، اما از آنجایی که اکثر این برنامه‌ها صرفاً نرم‌افزارهایی با توانایی‌های محدودی هستند و در هر شرایطی قابل استفاده نیستند، خطر چندان جدی، کاربران را تهدید نمی‌کند، مگر آنکه یکی از این دوستان قصد کمی سربه‌سر گذاشتن با افراد را داشته باشد، زیرا هیچ‌یک از اینها، در حد آن کارهای بزرگی که می‌شنویم نیستند، هکرهای واقعی از سطح دانش بسیار بالایی برخوردارند و علاوه بر آن با استفاده از یک برنامه ۲۵۰۰ تومانی که یک دستفروش کنار خیابان می‌فروشد، نمی‌توان سایت یک مرکز بزرگ را که هزینه بسیار زیادی تنها برای تأمین امنیتش به کارشناسان می‌پردازد، هک کرد.

گرچه این خطرات در اکثر موارد، خیلی جدی نبوده و بیشتر جنبه شوخی دارند، اما در مواردی نیز می‌توانند بسیار آزاردهنده و ضرررسان باشند، نظیر آنچه درباره قفل‌شکنی نرم‌افزارها رخ می‌دهد. علاوه بر اینها، استفاده از بسیاری از این برنامه‌ها، به ضرر خود کاربران تمام می‌شود، زیرا برخی از آنها به‌گونه‌ای طراحی شده‌اند که پس از استفاده در سیستم کاربر، به‌صورت Back Door عمل کرده و برحسب نوع طراحی‌شان اطلاعات موردنظر طراح را از سیستم شما گرفته و بیرون می‌فرستند که این می‌تواند از مشخصات اشتراک اینترنت تا بسیاری چیزهای دیگر باشد.

البته با وجود وفور چنین برنامه‌های غیرقانونی در بازار تهران، اما هیچ‌گونه برخوردی با آنها صورت نمی‌گیرد.(۸)

۹ـ دستگیری جاسوسان اینترنتی در ایران

استفاده از اینترنت به‌منظور انتقال اطلاعات حساس نظامی و امنیتی به دشمن، یکی از روش‌های جدید سازمان‌های جاسوسی دنیاست، اما اولین‌بار است که اعلام می‌شود چند نظامی در ایران به اتهام جاسوسی اینترنتی دستگیر شده‌اند.

حجت‌الاسلام والمسلمین نیازی، رئیس سازمان قضایی نیروهای مسلح در تاریخ

۱۵/دی‌ماه/۱۳۸۲ در همایش روحانیون نیروهای مسلح استان خراسان در مشهد با اعلام این مطلب که امروز استراتژی دشمن برای براندازی نظام، استحاله از درون، ایجاد اختلاف، تفرقه و تضعیف اعتقادات دینی و مذهبی است، سعی می‌کند این استراتژی را در بین نیروهای مسلح به‌کار گیرد، گفت: «اخیراً چند نفر نظامی به اتهام جاسوسی اینترنتی در ایران دستگیر شده‌اند». وی افزود؛ این افراد با استفاده از اینترنت اطلاعات و اخباری را با سازمان سیا CIA (سازمان اطلاعات مرکزی آمریکا) رد و بدل کرده‌اند، اما توضیح بیشتری در این زمینه ارائه نکرد.[۹]

۱۰ـ امنیت شبکه در ایران

پس از حمله گسترده و بی‌سابقه به سایت‌های ایرانی در تابستان ۱۳۸۱ توسط هکری که خود را مرد عنکبوتی می‌نامید، بحث امنیت شبکه در ایران برای اولین‌بار در مطبوعات و محافل اینترنتی کشور مطرح گشت. این اتفاق اگرچه ممکن بود در هر جای دنیا و با وجود امن‌ترین سیستم‌های کامپیوتری نیز به‌وقوع بپیوندد، اما در ایران و در میان کاربران ایرانی که به تازگی با محیط نامأنوس اینترنت انس و الفت گرفته‌اند و از سد اینترنت گذشته‌اند، کمی بغرنج و مسئله‌ساز شد. پس از این حمله، برخی از محافل مطبوعاتی با موضع‌گیری در قبال سطح پایین امنیت (Server)ها و شبکه‌های ایرانی به اظهارنظر و تحلیل در این زمینه پرداختند و برخی از کارشناسان نیز با بررسی علمی کم و کیف و راه‌کارهای افزایش امنیت شبکه‌ها تلاش کردند تا به نقش‌نمایی در این خصوص بپردازد. یکی از ایده‌های مطرح و قابل تأمل در این مورد آن است که امنیت شبکه‌ها و سرورهای ایرانی تا حدود بسیاری به استانداردها و ایده‌آل‌های جهانی امنیت شبکه نزدیک است و فاصله‌ای قهقرایی با این موضوع ندارد، اما سطح امنیت شبکه‌ای حاکم بر سایت‌های ایرانی به حدی است که یک هکر می‌تواند با کمی زحمت به آنها نفوذ کرده و باعث اختلال در عملکردشان شود، به همین دلیل است که نیاز آنها به مقوله امنیت نیازی جدی و در سطح بالا نیست، بلکه واقعیت این است که سطح امنیت در شبکه‌های جهان را می‌توان به ۲ دسته مختلف تقسیم کرد؛

۱. دسته اول، امنیت سایت‌هایی است که به‌دلیل نوع و ماهیتی که دارند از لحاظ امنیتی چندان حائز اهمیت نیستند. این گروه سایت‌هایی را شامل می‌شود که از کنش‌های مالی و نقل و انتقال اطلاعات محرمانه نظامی و غیره برخوردار نبوده و بیشتر در زمینه‌های اطلاع‌رسانی و تبلیغاتی فعال هستند. بدیهی است نفوذ به این قبیل سایت‌ها برای هکرها و سارقان اینترنتی استفاده چندانی نداشته و در واقع یک نوع تلاش عبث به‌شمار می‌آید. البته سایت‌هایی این‌چنینی معمولاً توسط هکرهایی مورد حمله قرار می‌گیرند که به‌دلایل خاصی از این اقدام خود اهدافی جز ارضای شخصی و یا تسویه حساب ندارند. شاید بتوان به هکرهای این قبیل سایت‌ها، هکرهای بیمار گفت! از طرفی حمله به چنین سایت‌هایی در حالت کلی نمی‌تواند خسارات سنگین و یا سوءاستفاده‌های مالی به‌دنبال داشته باشد. در نتیجه، اعمال شیوه‌های سطح بالای حفظ امنیت بیش از آنکه برای صاحبان سایت‌ها مفید باشد، هزینه‌ساز و غیراقتصادی است. در حال حاضر بالای ۹۰ درصد از سایت‌های ایرانی را این گروه از سایت‌ها تشکیل می‌دهند.

۲. دسته دوم، سایت‌های سیستم‌های بانکی، مراکز حساس نظامی و امنیتی است که می‌توانند انگیزه‌های بسیاری را برای نفوذگران ایجاد نمایند. بیشتر حمله‌کنندگان به این گروه از سایت‌ها را افرادی تشکیل می‌دهند که در پی اغراض سیاسی، جاسوسی و یا سوءاستفاده مالی هستند. برای نمونه، اکثر قریب به اتفاق هکرها از حمله به سایت‌هایی که دارای کنش‌های مالی هستند، هدفی جز به سرقت بردن اطلاعات مالی، نظیر شماره کارت اعتباری یا اختلاس و جابه‌جایی پول و انتقال آن به حساب خود ندارند و یا حمله‌کنندگان به مراکز اطلاعاتی و نظامی به‌دنبال اهداف سیاسی یا سرقت اطلاعات محرمانه آن مراکز هستند. در این حالت، طبیعی است که سیستم‌های امنیتی این قبیل سایت‌ها باید از سطح امنیتی بسیار بالایی برای حفظ امنیت خود برخوردار باشند. در نتیجه، صرف هزینه‌های گزاف استفاده از این سطح امنیت برای آنها از توجیه اقتصادی برخوردار است.

باتوجه به اینکه در ایران هنوز سیستم‌های مربوط به کارت اعتباری الکترونیکی، بانکداری

الکترونیکی و تجارت الکترونیکی، متداول نشده است، فعلاً در این بخش نگرانی خاصی وجود ندارد و هک و نفوذ و خرابکاری‌های اینترنتی بیشتر به سایت‌های خدمات‌رسان، خبری یا وبلاگ‌ها و ایمیل‌ها اختصاص دارد.

از سوی دیگر، سطح امنیتی سرورها و شبکه‌های ایرانی با توجه به هزینه‌هایی که از کاربران خود دریافت می‌کنند، نسبتاً متناسب است و در بروز چنین حملاتی نباید از سیستم‌های امنیتی سرویس‌دهندگان اینترنتی و فروشندگان فضا در اینترنت توقع بیشتری داشت.(۱۰)

۱۱ـ ایران و جنگ الکترونیک

به عقیده مهندس محمدرضا مولوی، عضو هیأت علمی و مدیر گروه مخابرات دانشکده پست و مخابرات، احساس می‌شود مسئله جنگ الکترونیک و نحوه رویارویی با آن به فراموشی سپرده شده و تنها در حد یک سری مسائل تئوریک مطرح می‌شود. در حالیکه این مسئله در هر زمان، عاملی مخاطره‌برانگیز است. با توجه به جنگ در منطقه و حمله تنها ابرقدرت جهان یعنی آمریکا و متحدش انگلیس به عراق، ما باید بتوانیم در خصوص تجهیزات الکترونیکی در ایران و به روز کردن آنها، تجدیدنظر عمده‌ای انجام دهیم. همچنین ضروری است، مراکز تحقیقاتی نیز مانند دوران جنگ فعالیت بیشتری در این زمینه داشته باشند. در زمینه جنگ الکترونیک[1] توجه به نیروی متخصص انسانی و آموزش آنها از اهمیت بسزایی برخوردار است، چراکه با چنین زمینه فعلی علم در جنگ الکترونیک در میان کشورها سخنی برای گفتن نداریم. در مسئله خرید سخت‌افزار نیز باید همگام با آن مسائل، تحقیقاتی صورت گیرد.

کشورهای صاحب تکنولوژی در فروش تجهیزات خود، بخش‌های اصلی را نزد خود نگاه می‌دارند. در نهایت باید به موازات خرید تجهیزات تکنولوژیک، نیروی انسانی آموزش دیده و نحوه تعمیرات و پشتیبانی قطعات را نیز مدنظر قرار دهیم. همواره در کشورها از جمله آمریکا، بهترین متخصصان در سیستم‌های نظامی و امنیتی کار می‌کنند و به نحو مطلوبی نیز از طرف

---

1. Electronic Warfare

دولت حمایت می‌شوند. درباره روند نفوذ در سیستم‌های موجود، آمریکایی‌ها و سایر کشورهای غربی که امکان پرتاب ماهواره در مدار نزدیک زمین را دارند، ماهواره‌های جاسوسی خود را در مدار ۳۰۰ کیلومتری زمین قرار می‌دهند. حتی اگر در تجهیزات فروخته شده به سایر کشورها، با نصب یک IC کوچک در سیستم، می‌توانند امواج آنرا از طریق ماهواره دریافت کنند. البته این مطلب از لحاظ تئوری قابل قبول است، اما از نظر علمی، توضیحات شفافی در این زمینه وجود ندارد. حساسیت عملیات جاسوسی[1] و امنیت سیستم‌ها[2] در حدی است که حتی اینترنت که در ابتدا مربوط به ارتش آمریکا بوده نیز شبکه‌ای قابل شنود و کنترل است و به این لحاظ کشورهای پیشرفته، از سایت‌های خاص با امنیت بالا استفاده می‌کنند که راه نفوذ به آنها بسیار مشکل است. با پیشرفت تکنولوژی، کشورهای عقب‌مانده بیشتر حالت انفعالی می‌گیرند و با ورود تجهیزات پیشرفته در صورت آشنا نبودن با علم و جزئیات آنها، تنها واردکننده هستند و به‌طور قطع از نظر امنیتی، تجهیزات آنها زیر سؤال می‌رود.[(۱۱)]

۱۲ـ جرائم رایانه‌ای در ایران

در حال حاضر، کمیته ویژه بررسی جرائم کامپیوتری و اینترنتی در دبیرخانه شورای عالی قضایی تشکیل شده است. یک سال پیش همایشی در این زمینه برگزار گردید و طی آن قرار بود راه‌کارهای قانونی برای مقابله با جرائم کامپیوتری را تدوین کنند. با گذشت یک سال، گروهی از دست‌اندرکاران در جلسه‌ای راهکارهای حل مسائل کوتاه‌مدت را مورد بررسی قرار دادند و قرار است اجرای این برنامه از طریق آموزش کادر قضایی و انتظامی آغاز شود. بنا بر گزارشی که از این جلسه منتشر شده است، کمیته‌های فرعی کار تدوین قوانین و مسائل بلندمدت را پیگیری خواهند کرد.

هنوز جرائم کامپیوتری در ایران چندان گسترده نیست و نمی‌توان به درستی گفت که اولین جرم کامپیوتری در ایران چه زمانی اتفاق افتاده است.

---

1. Espionage Operation
2. Security System

اولین جرم

اما اولین جرم کامپیوتری ایران در روز ۲۶ خرداد ۱۳۷۸ به ثبت رسیده است که در آن، یک دانشجوی کامپیوتر و یک کارگر چاپخانه در کرمان، چک‌های تضمینی را جعل می‌کردند.

پس از آن موارد دیگری نیز در این رابطه به‌عنوان جرم کامپیوتری به ثبت رسیده که مهم‌ترین آنها اختلاس بوده است. جعل اسکناس، اسناد و بلیت‌های شرکت‌های اتوبوسرانی، جعل اسناد دولتی، از قبیل گواهی‌نامه رانندگی، کارت پایان خدمت، مدارک تحصیلی، اوراق خرید و فروش خودرو و موتور سیکلت، جعل چک‌های مسافرتی و عادی نمونه‌هایی از جرائم کامپیوتری در ایران هستند. اما گاهی موضوع از اختلاس و جعل اسناد معتبر دولتی فراتر رفته است. در سال ۱۳۸۲، خبر حمله به چند سایت در ایران منتشر شد. سایت ماهنامه دنیای کامپیوتر، سایت مجله دنیای ارتباطات و کامپیوتر، سایت گالری الهه، سایت برترین‌های وبلاگ‌نویسی در ایران، از جمله سایت‌هایی بوده که توسط «گروه مش‌قاسم» مورد نفوذ قرار گرفته و تخریب شد.

به‌نظر می‌رسد، حمله به سایت‌های اینترنتی بیشتر به قصد نشان دادن ضعف‌های امنیتی سرورها و سایت‌های ایرانی صورت گرفته است.

موانع پیگیری

مقابله با جرائم اینترنتی به هیچ عنوان ساده نیست. به فرض دستگیری فرد خاطی، باز هم قاضی در صدور حکم با موانع قانونی مواجه است. کارشناسان می‌گویند؛ مشکل در آن است که در ایران، نه قانونی در این زمینه وجود دارد و نه افرادی که بتوانند به تحقیق بپردازند یا در مقام قاضی، در مورد آن حکم صادر کنند.

البته این مشکل فقط مربوط به ضعف قوانین نیست، بلکه پلیس هم در این زمینه آموزشی ندیده است. چندان‌که اگر فردی از طریق پست الکترونیکی در قبال آزادی فرد دیگری باج‌خواهی کند، ردیابی فرد خاطی بدون آموزش مأموران پلیس ممکن نیست و به‌نظر نمی‌رسد

مورد مسائل و سؤالات کلیدی که این استراتژی باید به آنها بپردازد، جویا شد. سپس سؤالات گردآوری شده در صفحات وب ارگان‌های دولتی، انجمن‌ها و سازمان‌های خصوصی قرار گرفت. شهروندان بسیاری نظراتشان را ارائه دادند. این پیش‌نویس استراتژی، پاسخ‌هایی برای اکثر سؤالات مطرح‌شده ارائه داده و باقی سؤالات را جهت بحث و تبادل‌نظر بیشتر در «کادرهای برنامه کاری» قرار می‌دهد.

به‌منظور گفت‌وگوی ملی بیشتر، «هیأت حفاظت زیرساخت‌های حیاتی» منصوب‌شده توسط ریاست‌جمهوری، جلساتی عمومی در بهار ۲۰۰۲ پیش از انتشار استراتژی حاضر برگزار کرد. این جلسات در شهرهای گوشه و کنار کشور برگزار گردید.

علاوه بر این، دفتر «امنیت زیرساخت‌های حیاتی» (CIAO) وزارت بازرگانی، جلساتی با مقامات دولت ایالتی و محلی ایالات متعدد برگزار کرد که شامل کنفرانس‌های ملی در آستن تگزاس در تاریخ ۱۲ الی ۱۳ فوریه ۲۰۰۲ و پرینستون نیوجرسی در تاریخ ۲۳ الی ۲۴ آوریل ۲۰۰۲ بود. پیرو انتشار این استراتژی بر روی اینترنت، جلسات و گردهمایی‌های شهری و ایالتی دیگری هم ممکن است جهت ادامه گفت‌وگوی ملی در باب تأمین امنیت اینترنتی برگزار گردد. جزئیات بیشتر در این زمینه در وب سایت http://www.secure-cyberspace.gov اعلام خواهد شد.

استراتژی ملی امنیت اینترنتی، مکمل سایر استراتژی‌هاست.

«استراتژی ملی امنیت اینترنتی» مکمل «استراتژی ملی امنیت داخلی» و «استراتژی امنیت ملی ایالات‌متحده» است. بخش «سیاست‌ها و اصول» همراه با فرمان اجرایی رئیس‌جمهور بوش، راهنمای سیاست دولت در امنیت اینترنتی است.

شهرهایی که جلسات عمومی در آنها برگزار شده؛

دنوور، کلرادو

شیکاگو، ایلینویز

استراتژی به‌عنوان فرآیندی مستمر

این استراتژی به‌منزله وحی منزل نیست. «هیأت حفاظت از زیرساخت‌های حیاتی» (PCIPB) که از سوی رئیس‌جمهور منصوب شده‌اند، قصد دارند تا به‌صورت دوره‌ای، نگارش‌های جدیدتر و کامل‌تر استراتژی حاضر را به‌صورت برخط منتشر سازند. مقدمه هر یک از نگارش‌ها، مطالب به هنگام شده از نگارش قبلی را مشخص می‌سازد.

اجزای این استراتژی توسط ذی‌نفعان و کاربران اینترنت تهیه و تنظیم شده است. نمایندگان شرکت‌های صاحب زیرساخت‌های حیاتی و شرکت‌های اداره‌کننده این زیرساخت‌ها گردهم آمده و پیش‌نویس طرح چگونگی تأمین امنیت اینترنتی در بخش‌های مربوطه، اعم از بانکداری و امور مالی، برق، راه‌آهن و سایر بخش‌ها را تهیه کرده‌اند. کالج‌های محلی و دانشگاه‌های بزرگ به همراه یکدیگر برای تأمین امنیت اینترنتی در مؤسسات آموزش عالی برنامه‌ریزی‌هایی کرده‌اند. پلیس شهرهای بزرگ و کلانتری‌های شهرهای کوچک دست به دست یکدیگر داده و به همکاری در تأمین نیازمندی‌های امنیت اینترنتی برای نیروهای انتظامی پرداخته‌اند. کمیسیون‌های هر دو مجلس جلساتی درباره امنیت اینترنت و عناوین مربوطه آن برگزار کرده‌اند. انجمن‌های ملی جلسات متعددی داشته و هزاران ساعت از زمان خود را در جهت تلاش برای تکامل این استراتژی وقف کرده‌اند.

این گروه‌ها، استراتژی‌هایی به‌منظور کمک به تأمین امنیت در بخش‌های مربوطه خود از اینترنت که تحت مالکیت یا مدیریت آنهاست تهیه و تنظیم کرده‌اند، چراکه هر کاربر اینترنت باید وظیفه خود در تأمین امنیت آن‌را ادا کند و در عین حال این مسئله باعث نمی‌شود تا دولت فدرال از مسئولیت‌های خود معاف گردد. این مسئولیت‌ها که تعدادشان کم هم نیست در استراتژی حاضر مشخص شده‌اند. اما در عین حال خاطرنشان می‌کند که دولت فدرال به تنهایی نمی‌تواند امنیت اینترنت را تأمین کند. ما همه باید وظیفه خود را ادا کنیم و به‌خاطر داشته باشیم که موفقیت این استراتژی به تلاش‌های تک‌تک افراد ملت بستگی خواهد داشت.

برای تشویق بحث و تبادل‌نظر، هیأت منصوب شده، نظرات متخصصان سراسر کشور در

استراتژی به‌عنوان جایگاه طرح نظرات

این سند به همراه مطالب «برخط» (Online) از بخش خصوصی و دانشگاه‌ها، بیانگر استراتژی اجرایی ایالات‌متحده برای تأمین امنیت سیستم‌ها و شبکه‌های فناوری اطلاعات است که در عملیات اقتصاد ملی، سیستم دفاعی و خدمات اساسی نقش حیاتی ایفا می‌کنند. این شبکه‌ها، تجهیزات و نرم‌افزار فناوری اطلاعات مربوطه آنها، فضای قلمرو اینترنتی ما را تشکیل می‌دهند.

استراتژی حاضر، دارای جایگاهی است تا اقشار مختلف ملت ما، برنامه‌ها و استراتژی خویش را برای تأمین امنیت بخش خود از فضای اینترنتی مطرح سازند. در این استراتژی، خوانندگان برنامه‌های اقشار مختلف ملت آمریکا از جمله: معلمان، افسران نظامی، متخصصان امنیت، پزشکان، دلالان سهام، پلیس، کارمندان دولت، دانشمندان علوم رایانه‌ای، مقامات دولت ایالتی، مدیران شرکت‌ها مقامات فدرال را ملاحظه می‌کنند.

استراتژی مذکور با موارد زیر تکامل خواهد یافت:

- تهیه استراتژی‌هایی از سوی کشور برای تأمین امنیت بخش‌های مختلف اینترنت؛
- تشریح بیشتر و تصحیح استراتژی‌های فرعی در اثر کسب تجارب؛
- تغییر فناوری و به‌تبع آن ایجاد چالش‌ها و توانایی‌های جدید؛
- دانش بیشتر در مورد تهدیدات و نقاط آسیب‌پذیر که به‌طور دائم در حال تغییرند؛
- حصول اتفاق‌نظر درباره نظراتی که در نسخه‌های منتشره قبلی برای مباحثه پیشنهاد شده‌اند؛
- تکامل برخی از نظرات ابتدایی.

مردم آمریکا اعم از کاربر خانگی[1] اینترنت، صاحب کسب و کار کوچک، مدیر اطلاعات شرکت، شهردار شهر، فرماندار ایالت، مدیرعاملان شرکت‌های رده بالا یا یک عضو هیأت مدیره شرکتی می‌توانند برای راهنمایی و توصیه به اینجا مراجعه کنند.

1. Home User

ـ استراتژی ملی امنیت اطلاعات و اینترنت آمریکا ـ سال ۲۰۰۳

گزارش زیر ترجمه و تلخیص بخشی از استراتژی جدید دولت آمریکا در زمینه امنیت اطلاعات و اینترنت است.

دولت آمریکا با توجه دقیق به اهمیت نقش استراتژیک و بسیار حیاتی فناوری ارتباطات و اطلاعات، توسعه کاربری این فناوری را به‌عنوان محور امنیت ملی اعلام و در این راه هزینه بسیاری را برای تمهید زیرساخت‌های موردنیاز صرف نموده است. یکی از مهم‌ترین این زیرساخت‌ها که خصوصاً در شرایط بسیار متفاوت و متحول شده پس از حادثه ۱۱ سپتامبر توجه مضاعفی را به خود معطوف کرده، امنیت اطلاعات و اینترنت است. دولت آمریکا در گزارش زیر فرآیند شکل‌گیری استراتژی ملی خود در این زمینه، از جمله فراخوان عمومی برای اعلام‌نظر و نقد برنامه‌های خود را تشریح کرده است.

مقدمه

«استراتژی ملی امنیت داخلی» آمریکا به یک تهدید بسیار خاص و جدی یعنی تروریسم در ایالات‌متحده می‌پردازد و چارچوبی جامع برای ساماندهی تلاش سازمان‌های فدرال، ایالتی، محلی و خصوصی که غالباً کارکردهای اصلی آنها ارتباطی با امنیت ملی ندارد، ارائه می‌دهد. اینترنت برای امنیت داخلی و امنیت ملی، حیاتی است. امنیت و قابلیت اطمینان اینترنت، ضامن اقتصاد، زیرساخت‌های حیاتی و تشکیلات دفاع ملی است. «استراتژی ملی امنیت اینترنتی» استراتژی اجرایی جهت پشتیبانی از «استراتژی ملی امنیت داخلی» و «استراتژی ملی امنیت ایالات‌متحده» است.

«استراتژی ملی امنیت اینترنتی» طرح‌هایی با هدف تأمین امنیت سیستم‌های اطلاعات آمریکا در مقابل اختلال و تخریب عمدی و خطرناک و افزایش آمادگی ملی در این خصوص را شامل می‌شود. این استراتژی به همراه استراتژی تکمیلی «حفاظت فیزیکی امنیت داخلی»، مبنای استراتژیک تلاش‌های ملت برای حفاظت از زیرساخت‌هایش را تشکیل می‌دهد.

نمونه‌ای از گردهمایی‌های موجود در برخی از کشورهای عضو اتحادیه است. هر کجا که چنین گردهمایی‌هایی وجود نداشته باشند، کمیسیون، کشورهای عضو اتحادیه را به برپایی آنها ترغیب می‌کند و همکاری گسترده بین این گردهمایی‌های مختلف توسط گردهمایی اتحادیه اروپا تقویت و تسهیل خواهد شد.

کمیسیون همچنان به ارتقای امنیت و اعتماد در طرح اروپای الکترونیکی، طرح اجرایی اینترنت، (برنامهٔ IST فناوری‌های جامعهٔ اطلاعاتی) و برنامهٔ چارچوبی بعدی برای RTD ادامه خواهد داد. این کار، شامل افزایش محصولات و خدمات اینترنتی با میزان متناسبی از امنیت و استفاده آزادانه‌تر از محصولات پیشرفتهٔ رمزنگاری همراه می‌باشد که از طریق مذاکره و تبادل‌نظر بین تمام گروه‌های ذی‌نفع، انجام می‌پذیرد.

کمیسیون، پروژه‌های بیشتری را در خلال برنامه‌های موجود جهت حمایت از آموزش پرسنل مراکز انتظامی، مباحث مربوط به جرائم اینترنتی و حمایت از انجام تحقیقات در محاسبات حقوقی، راه‌اندازی خواهد کرد.

کمیسیون همچنین تأمین اعتبار برای بهبود محتوا و قابلیت استفادهٔ از پایگاه اطلاعاتی قوانین داخلی کشورهای عضو اتحادیه را که به‌دنبال مطالعهٔ COMCRIME احداث شده است، بررسی خواهد کرد و مطالعه‌ای هم جهت ارائه تصویری بهتر از ماهیت و دامنهٔ جرائم مرتبط با رایانه در کشورهای عضو اتحادیه انجام خواهد داد.

عملکرد دیگر گردهمایی‌های بین‌المللی

کمیسیون همچنان به ایفای نقشی کامل در ایجاد همکاری بین کشورهای عضو اتحادیه در دیگر گردهمایی‌های بین‌المللی مانند شورای اروپا و گروه ۸ ادامه می‌دهد. اقدامات کمیسیون در سطح اتحادیهٔ اروپا، پیشرفت حاصله در دیگر گردهمایی‌های بین‌المللی را به‌طور کامل درنظر آورده و بر مبنای آن سعی در همسان‌سازی قوانین در سطح اتحادیهٔ اروپا دارد.

اروپا که دربرگیرندهٔ هر دو نوع نژادپرستی و بیگانه‌ستیزی اینترنتی و غیراینترنتی می‌باشد، تلاش خواهد کرد و سرانجام مسئلهٔ قاچاق موادمخدر در اینترنت نیز مورد بررسی قرار خواهد گرفت.

ـ به‌کارگیری اصل شناسایی متقابل قواعد انتظامی پیش از محاکمه؛ در مورد پی‌جویی جرائم اینترنتی و پیشبرد پیگردهای کیفری مرتبط با جرائم رایانه‌ای که بیش از یک کشور عضو اتحادیه را شامل شود و در عین حال نیز تأمین قانونی متناسب در مورد حقوق اساسی فرد را دربرداشته باشد که این به لزوم بررسی طرح‌های پیشنهادی در مورد به‌دست آوردن و تثبیت ادله اشاره دارد.

ـ در میان سایر موارد رایزنی، لزوم اتخاذ هرگونه موازینی، به‌خصوص با ماهیت قانونگذاری در خصوص نگهداری اطلاعات مبادله شده، توسط کمیسیون اروپایی و بر مبنای دستاورد فعالیت‌هایی که در گردهمایی اتحادیه اروپا در این زمینه مطرح و انجام خواهند شد، بررسی می‌شود.

طرح‌های پیشنهادی غیرتقنینی

لزوم عملکرد در موارد یادشده ذیل؛

کمیسیون کار تشکیل و ریاست گردهمایی در اتحادیه اروپا را برعهده گرفته است که در آن مراکز انتظامی، تأمین‌کنندگان خدمات اینترنت، عوامل اجرایی شبکه، گروه‌های مصرف‌کننده و مراجع حفاظت اطلاعات به‌منظور افزایش همکاری‌ها در سطح اتحادیه اروپا گردهم می‌آیند.

آنان این کار را با ۱. ارتقای سطح آگاهی عمومی از خطراتی که اعمال کیفری می‌تواند در اینترنت به‌وجود آورد، ۲. تقویت بهترین راهکارهایی که برای امنیت فناوری اطلاعات لازم است، ۳. توسعهٔ ابزار و راهکارهای مؤثر ضدجرم برای مقابله با جرائم مربوط به رایانه، ۴. گسترش بیشتر مکانیسم‌های هشدار قبل از وقوع و مدیریت ریسک، انجام می‌دهند. این طرح

استراتژیک در این کار به گردآوری فناوری‌های مقرون به صرفه و کارآمد و دیگر فناوری‌های اعتمادآفرین و اقدامات سیاستگذاری اتحادیه اروپا، معطوف است.

ولیکن، هر اقدامی که مورد توافق اتحادیه اروپا قرار می‌گیرد، باید کشورهای داوطلب در حوزهٔ اتحادیه را نیز شامل شود و همکاری‌های بین‌المللی را هم گسترش دهد تا سایر کشورها به پناهگاهی امن برای مرتکبان جرائم رایانه‌ای تبدیل نگردند. بنابراین باید لزوم شرکت نمایندگانی از این کشورها در تمام یا برخی از جلسات مربوط به اتحادیه اروپا را بررسی کرد. طرح‌های پیشنهادی کمیسیون را می‌توان به موارد ذیل تقسیم نمود؛

طرح‌های پیشنهادی برای قانونگذاری

کمیسیون طرح‌هایی برای قانونگذاری تحت بند VI از معاهدهٔ اتحادیهٔ اروپا ارائه خواهد کرد؛

ـ طرح‌هایی برای یکسان‌سازی قوانین کشورهای عضو اتحادیه در مورد جرائمی چون هرزه‌نگاری کودکان؛ این طرح بخشی از مجموعه طرح‌های پیشنهادی شامل، مباحث گسترده‌تری در مورد سوءاستفادهٔ جنسی از کودکان و قاچاق انسان است که در بیانیهٔ کمیسیون در دسامبر ۱۹۹۸ راجع‌به قاچاق انسان مطرح شده‌اند. این طرح، کاملاً در راستای تلاش‌های پارلمان اروپا در تبدیل اقدامات اتریش (کسب مصوبه‌ای از سوی شورا در مورد هرزه‌نگاری کودکان) است که مستلزم همسان‌سازی قوانین می‌باشد. همچنین با نتایج نشست تامپر و استراتژی اتحادیهٔ اروپایی برای مقابله با جرائم سازمان‌یافته در هزارهٔ جدید نیز هماهنگ است. این طرح بخشی از برنامهٔ اسکوربورد برای ایجاد حوزه‌ای از آزادی، امنیت و عدالت است.

ـ یکسان‌سازی بیشتر قوانین ماهوی کیفری در حوزهٔ جرائم مربوط به فناوری پیشرفته؛ این طرح، (جرائم مربوط به نفوذ در سیستم) (Denial of Service Attacks, Hacking) را نیز دربرمی‌گیرد. همچنین کمیسیون دامنهٔ عملکرد علیه نژادپرستی و بیگانه‌ستیزی در اینترنت را خواهد سنجید و در عین حال جهت تصویب چارچوبی براساس بند VI از معاهدهٔ اتحادیه

مورد حقوق بشر انجام دهند. کمیسیون بر این باور است که توافق حاصله در مورد امکان شنود در کنوانسیون همیاری دوجانبه در مسائل کیفری، حداکثر توافق قابل حصول و ممکن در حال حاضر است. کمیسیون اجرای این توافق را با اعضای اتحادیه، بخش صنعت و کاربران همچنان مورد بازنگری قرار خواهد داد تا این اطمینان حاصل شود که اقدامات مؤثر، شفاف و متوازن هستند.

ـ وجود پرسنل آموزش‌دیده و مجهز کافی در میان مجریان قانون، همکاری نزدیک با تأمین‌کنندگان خدمات اینترنتی و عوامل ارتباطات راه دور در زمینهٔ آموزش در آینده بیش از پیش تقویت خواهد شد.

ـ همکاری مناسب میان تمام عوامل دخیل شامل؛ کاربران و مصرف‌کنندگان بخش صنعت، مراکز انتظامی و حفاظت اطلاعات. این کار برای پی‌جویی جرائم رایانه‌ای و حفظ امنیت عمومی ضروری است. بخش صنعت باید در چارچوب وظایف و ضوابط مشخص عمل کند. دولت‌ها باید بدانند که نیازهای مجریان قانون ممکن است موانعی برای بخش صنعت به‌وجود آورد، بنابراین باید با اقدامات مناسب، سعی در به حداقل رساندن این موانع کنند. در عین حال، بخش صنعت هم باید در فرآیندهای تجاری خود ملاحظات مربوط به امنیت عمومی را در نظر بگیرد. این کار بیش از همه نیازمند همکاری مؤثر و حمایت کاربران شخصی و مصرف‌کنندگان می‌باشد.

ـ اقدامات مستمر بخش صنعت و گروه‌های هدایت‌شده از سوی اجتماع؛ خطوط تلفن قرمز، که مدتی است برای گزارش موارد انتشار مطالب غیرمجاز و مضر بر روی اینترنت راه‌اندازی شده‌اند، ممکن است به دیگر سوءاستفاده‌ها نیز گسترش یابند. نظارت مستقل بخش صنعت و یک یادداشت تفاهم چندجانبه می‌تواند بیشترین تعداد گروه‌های ذی‌نفع را گردهم آورده و نقشی چندجانبه در کمک به پیشگیری و مقابله با جرائم رایانه‌ای و افزایش آگاهی و اعتماد افراد داشته باشد.

ـ دستاوردها و قابلیت‌های بالقوه R&D باید تا بیشترین حد ممکن به‌کار گرفته شود؛ توجه

مرکز مشترک پژوهشی کمیسیون که از اقدام سنجش قابلیت اعتماد در برنامهٔ (IST فناوری‌های جامعهٔ اطلاعات) حمایت می‌کند، تلاش‌های خود را بر توسعه ابزارها، شاخص‌ها و آمار متناسب و همسو در رایزنی با دیگر احزاب و گروه‌های ذی‌نفع، ازجمله یوروپول معطوف خواهد داشت. این کار با هدف ایجاد یک دسته‌بندی و فهم مناسب از فعالیت‌های غیرمجاز، توزیع جغرافیایی این فعالیت‌ها، میزان رشد آنها و کارایی اقداماتی که جهت مقابله با آنها صورت می‌گیرد، انجام می‌شود. در صورت ضرورت، مرکز مشترک پژوهشی کمیسیون، بار دیگر با گروه‌های پژوهشی همکاری کرده و نتایج تلاش‌های آنان را متحد می‌کند. همچنین با حفظ یک وب ـ سایت اینترنتی در این زمینه، میزان پیشرفت و عملکرد خود را به گردهمایی اتحادیهٔ اروپا گزارش می‌دهد.

نتایج و پیشنهادات

پیشگیری و مقابلهٔ مؤثر با جرائم رایانه‌ای مستلزم شرایط خاصی به شرح ذیل است؛

ـ دسترسی به فناوری‌های بازدارنده؛ این کار مستلزم وجود یک محیط نظارتی متناسب است که اختیار و انگیزهٔ مناسبی برای پژوهش و خلاقیت به‌وجود می‌آورد. حمایت مالی دولت را می‌توان برای حمایت از توسعه و به‌کارگیری فناوری‌های متناسب امنیتی موجه دانست.

ـ آگاهی از خطرات بالقوهٔ امنیتی و روش‌های مقابله با آنها

ـ وجود موازینی برای قانونگذاری ماهوی و شکلی با ملاحظه فعالیت‌های کیفری داخلی و بین‌المللی؛ قوانین ماهوی کیفری داخلی باید به میزان کافی برای تعقیب سوءاستفاده‌ها جامع و کارآمد باشند، امکان اعمال مجازات‌های بازدارنده را فراهم آورده و در رفع مشکلات جنایی دوجانبه و تسهیل همکاری‌های بین‌المللی مؤثر باشند. در صورت نیاز منطقی و ضروری مرکز انتظامی مجری قانون به تجسس، توقیف و ضبط سریع اطلاعات رایانه‌ای در درون حوزهٔ استحفاظی خود قوانین آیین دادرسی باید امکان این اقدامات را فراهم آورد و این کار را در چارچوب اصول و استثنائات خاص موجود در قوانین جمعی و طبق کنوانسیون اروپایی در

پروژه‌های RTD مورد حمایت اتحادیهٔ اروپا

در برنامهٔ RTD، فناوری‌های جامعهٔ اطلاعاتی (IST) که بخشی از پنجمین برنامهٔ اساسی بوده و از ۱۹۹۸ تا ۲۰۰۲ ادامه داشته بر توسعه و به‌کارگیری فناوری‌های اعتمادآفرین تأکید شده است. فناوری‌های اعتمادآفرین به نوبهٔ خود شامل فناوری‌های امنیت اطلاعات و شبکه و نیز ابزار و روش‌هایی برای جلوگیری از سوءاستفاده از حقوق بنیادین فرد نسبت به حریم شخصی خود، حفاظت از اطلاعات و دیگر حقوق فردی و مقابله با جرائم رایانه‌ای هستند.

برنامه به‌کارگیری فناوری‌های جامعهٔ اطلاعاتی، به‌خصوص در ارتباط با فناوری‌های امنیت شبکه و اطلاعات و دیگر فناوری‌های اعتمادآفرین در عملکرد کلیدی شماره ۲ ـ یعنی روش‌های جدید کار و تجارت الکترونیکی، چارچوبی را فراهم می‌سازد که هدف آن توسعهٔ قابلیت‌ها و فناوری‌های موجود برای شناسایی و مقابله با چالش‌های قریب‌الوقوع فناوری مربوط به پیشگیری و مقابله با جرائم رایانه‌ای بوده و تضمین می‌کند که الزامات حریم خصوصی و امنیتی را می‌توان در سطح اتحادیهٔ اروپا، جوامع مجازی رایانه‌ای و فردی به‌وجود آورد.

علاوه بر این، به‌منظور برخورد مناسب با چالش‌های مربوط به اعتماد و اطمینان، از قبیل پیشگیری و پی‌جویی جرائم رایانه‌ای، اقدامی جهت سنجش قابلیت اعتماد، در مورد برنامهٔ به‌کارگیری فناوری‌های جامعهٔ اطلاعاتی ترتیب داده شده است. نقش این اقدام، کمک به جلب و حفظ اعتماد و اطمینان در زیرساخت‌های بسیار به هم پیوسته اطلاعات و سیستم‌های شبکه‌ای است و این امر از طریق ارتقای آگاهی از قابل اعتماد بودن شبکه‌ها و به‌کارگیری فناوری‌های لازم برای ایجاد قابلیت اعتماد میسر می‌گردد. یک بخش لاینفک در این راستا، همکاری بین‌المللی است. برنامهٔ فناوری‌های جامعهٔ اطلاعاتی با سازمان‌های DARPA و NSF روابط کاری خود را توسعه داده و همچنین با همکاری وزارت امورخارجهٔ آمریکا، نیروی ضربت مشترکی برای مراقبت از زیرساخت‌هایی حیاتی تحت حمایت گروه مشاوران مشترک آمریکا/ اتحادیهٔ اروپا مربوط به توافق همکاری S&T، به‌وجود آورده است.

بین‌المللی، مانند شورای اروپا و کشورهای گروه ۸ در حال انجام است؛

ـ تقویت همکاری بین گروه‌های ذی‌نفع، شامل تبادلِ اصولی که بین مراکز انتظامی مجری قانون، بخش صنعت و کاربران مشترکند (مانند، شراکت‌نامهٔ همکاری متقابل و اصول کاری در راستای ضوابط حقوقی)

عملکردهای مستقیم بخش صنعت

مقابله با جرائم مرتبط با رایانه تا حدود زیادی به نفع جامعهٔ عظیم جهانی است. اگر بنا بر حفظ و جلب اعتماد مصرف‌کنندگان به تجارت الکترونیکی باشد، اقدامات لازم برای جلوگیری از جرائم مرتبط با اینترنت، باید بخش پذیرفته‌شده در امور تجاری محسوب شود. بسیاری از بخش‌های صنعتی، از قبیل بانکداری ارتباطات الکترونیکی، بخش کارت‌های عتباری و حق چاپ و نشر و مشتریان آنها قربانیان بالقوهٔ جرائم رایانه‌ای هستند.

شرکت‌ها به‌طور طبیعی از نام و علائم تجاری خود نگهداری کرده و بدین جهت در پیشگیری از کلاهبرداری نقش به‌سزایی ایفا می‌کنند. سازمان‌های ارائه‌کننده نرم‌افزار و صنایع صوتی (مانند صنعت فون گرافیک انگلیسی «BPI») گروه‌هایی را برای پی‌جویی سرقت (از قبیل سرقت‌های ادبی مرتبط با اینترنت) گماشته‌اند.

تأمین‌کنندگان خدمات اینترنتی در تعدادی از کشورهای عضو اتحادیهٔ اروپا، خطوط تلفن قرمزی برای گزارش انتشار مطالب غیرمجاز و زیان‌آور راه‌اندازی کرده‌اند. کمیسیون اروپا با تقویت برخی از این اقدامات در جهت مشارکت و برنامه‌های چارچوبی تحقیق و توسعه اتحادیه اروپا، طرح اجرایی اینترنت و بند پنجم از برنامه‌هایی مانند ایست[1] و دافنه[2] از آنها حمایت کرده و بهترین عملکرد در این مورد از طریق گردهمایی اتحادیهٔ اروپا تبادل می‌شود.

---

1. Stop

2. Daphne

نمایندگان مراکز انتظامی مجری قانون، تأمین‌کنندگان خدمات اینترنتی، عوامل ارتباطات راه دور، سازمان‌های آزادی مدنی، نمایندگان مصرف‌کنندگان (کاربران)، مراجع حفاظت اطلاعات و دیگر گروه‌های ذی‌نفع، به‌منظور گسترش بیشتر همکاری‌ها، برگزار نماید. در مرحلهٔ اول، این کار مسئولان دولتی را که از سوی کشورهای عضو اتحادیه، تعیین می‌شوند و سپس متخصصان فناوری و حریم خصوصی که در بند ۲۹ گروه کارگری، حفاظت اطلاعات متخصص شده‌اند و نمایندگان بخش صنعت و مصرف‌کنندگان با رایزنی نزدیک انجمن‌های صنعت و مصرف‌کننده را شامل می‌شود. در مرحلهٔ بعد، در این گردهمایی، نمایندگانی از کشورهای مرتبط جهت تبیین اقدامات مربوطه حضور خواهند داشت.

گردهمایی اتحادیهٔ اروپا به طریق علنی و شفاف عمل خواهد کرد و اسناد و مدارک مربوط به یک وب سایت را انتشار می‌دهد و تمام گروه‌های دخیل در آن به ارائه نقطه‌نظرات خود دعوت می‌شوند. این گردهمایی به‌طور اخص به مباحث زیر خواهد پرداخت؛

ـ ایجاد ارتباط‌های ۲۴ ساعته بین دولت و بخش صنعت در مناسب‌ترین مکان؛

ـ ایجاد شکل و ساختاری استاندارد و واحد برای ارسال تقاضای اطلاعات توسط مراکز انتظامی مجری قانون از بخش صنعت که باعث افزایش سطح استفادهٔ مراکز انتظامی از اینترنت در زمان ارتباط با تأمین‌کنندگان خدمات می‌شود؛

ـ ترغیب به توسعه و یا اجرای اصول رفتار یا بهترین عملکردها و تبادل چنین اصولی بین دولت‌ها و بخش صنعت؛

ـ تقویت تبادل اطلاعات پیرامون شیوه‌های جاری ارتکاب جرائم رایانه‌ای بین گروه‌های مختلف، به‌خصوص بخش صنعت و مراکز انتظامی مجری قانون و بررسی و اعمال خواسته‌های مراکز انتظامی در توسعهٔ فناوری‌های جدید؛

ـ تقویت روزافزون و توسعهٔ بیشتر سازوکارهای اخطار قبل از وقوع و مدیریت بحران برای جلوگیری، شناسایی و مواجهه با تهدیدات یا وقایع مخرب در زیرساخت‌های اطلاعاتی؛

ـ در صورت لزوم، ارائه همیاری تخصصی در مواردی که در شورا یا دیگر گردهمایی‌های

اجرایی (مانند، اتخاذ تصمیم در مورد اقدامات امنیتی مناسب) اهمیت دارد، بلکه برای اهداف بیمه‌ای نیز مطرح است.

یک پایگاه اطلاعاتی در مورد قوانین مربوط به جرائم رایانه‌ای که به‌عنوان بخشی از مطالعهٔ COMCRIME فراهم شده بود، در حال به روز شدن و قابل وصول شدن برای کمیسیون است. کمیسیون اصلاح مطالب (شامل قوانین، پرونده‌های دادگاهی و ادبیات تحقیق) و بهره‌وری این پایگاه اطلاعاتی[1] را بررسی خواهد کرد.

همکاری بین عوامل مختلف؛ گردهمایی اتحادیهٔ اروپا

همکاری مؤثر بین دولت و بخش صنعت در زمینه‌های حقوقی به‌عنوان عنصری اساسی در راهکار دولتی برای مقابله با جرائم مرتبط با رایانه، تلقی می‌شود. مجریان به عدم شفافیت کافی درخواست‌های خود از تأمین‌کنندگان خدمات اذعان دارند. نمایندگان بخش صنعت در کل از همکاری بهتر با مراکز انتظامی مجری قانون استقبال کرده و در عین حال همواره بر ایجاد یک توازن متناسب بین مراقبت از حقوق بنیادین و آزادی‌های شهروندان، به‌ویژه حق حریم خصوصی و لزوم مبارزه با جرائم و موانع اقتصادی که دامنگیر تأمین‌کنندگان خدمات شده، تأکید داشته‌اند.

مراکز انتظامی مجری قانون و بخش صنعت با همکاری یکدیگر می‌توانند سطح آگاهی عمومی نسبت به خطرات ناشی از خطاهای کیفری در اینترنت را بالا برده، بهترین راهکارها را برای حفظ امنیت تقویت کرده و به ایجاد ابزارها و رویکردهای مؤثر بر علیه جرم اقدام ورزند. تاکنون در برخی از کشورهای عضو اتحادیهٔ اروپا اقدامات مشابهی انجام گرفته که گردهمایی جرائم اینترنتی انگلستان با سابقه‌ترین و فراگیرترین آنها بوده است.

کمیسیون از این اقدامات استقبال کرده و خواستار تقویت آنها در تمام کشورهای عضو اتحادیه است. همچنین در نظر دارد یک گردهمایی در سطح اتحادیهٔ اروپا را با حضور

1. Web Site

تقبل کرده است. این دوره را می‌توان تا حدی‌که به‌طور اعم شامل جرائم مرتبط با رایانه شود، گسترش داد. اینترپول هم چند سالی است که در این راستا فعالیت‌هایی داشته که اقدامات آنرا در این زمینه می‌توان در مورد تعداد بیشتری از پرسنل اعمال کرد.

کشورهای عضو گروه ۸ نیز اقداماتی را ترتیب داده‌اند که زمینهٔ تبادل اطلاعات و تجارب بین مراکز انتظامی مجری قانون و ایجاد تکنیک‌های مشترک تعقیب بر مبنای موارد واقعی و مستدل را به‌وجود می‌آورند. در زمینه آموزش پرسنل، اقدام دیگری در نیمهٔ دوم سال ۲۰۰۱ صورت خواهد گرفت. کشورهای عضو اتحادیهٔ اروپا که عضو گروه ۸ هستند، می‌توانند این تجارب را در اختیار دیگر اعضای این اتحادیه قرار دهند.

در حوزه ویژهٔ مبارزه با هرزه‌نگاری کودکان در اینترنت، ایجاد و حفظ یک بایگانی مرکزی دیجیتال[1] متشکل از تصاویر هرزه‌نگاری کودکان در سطح بین‌المللی (که برای واحدهای تخصصی انتظامی در سطح داخلی با لحاظ کردن شروط لازم و محدودیت دسترسی و حفظ حریم خصوصی، بر روی اینترنت فراهم خواهد بود) به جست‌وجوی مجرمان و خرابکاران کمک نموده و در تعیین ماهیت جرم و آموزش افسران پلیس نیز مفید واقع می‌شود.

اطلاعات اصلاحی و مقررات مشترک برای حفظ سوابق

اقداماتی از قبیل، ایجاد یک مجموعه مقررات هماهنگ جهت حفظ اطلاعات ضبط‌شده برای پلیس و مراکز قضایی و نیز مجموعه‌ای از راهکارها برای تحلیل آماری جرائم رایانه‌ای به مراکز انتظامی مجری قانون و مراکز قضایی کمک خواهد کرد تا بهتر بتوانند به ذخیره‌سازی، تحلیل و ارزیابی اطلاعات رسمی که در این حوزهٔ متغیر به‌دست آمده، بپردازند.

این آمار و ارقام از دیدگاه بخش خصوصی نیز برای ارزیابی درست خطرات موجود و تحلیل سود و زیان مدیریت این ریسک‌ها لازم به‌نظر می‌رسند. این امر نه تنها به‌دلایل عملی و

---

1. Digital Central Archive

سخت‌افزارها برای این واحدها و آموزش پرسنل آنها هزینه‌های بسیاری دربرداشته و مستلزم تعیین اولویت‌ها و اتخاذ تصمیماتی سیاسی در سطوح متناسب دولتی است. تجارب واحدهای تأسیس‌شده در کشورهای عضو ارزش ویژه‌ای خواهد داشت و کمیسیون به تبادل این تجربیات کمک می‌کند.

کمیسیون همچنین معتقد است که یوروپول [پلیس اروپایی] می‌تواند از طریق هماهنگ‌سازی، تحلیل و دیگر کمک‌ها برای واحدهای تخصصی داخلی در سطح اتحادیهٔ اروپا، ارزش‌افزودهٔ بیشتری را فراهم آورد. لذا کمیسیون از توسعهٔ حوزهٔ اختیارات یوروپول برای پوشش جرائم رایانه‌ای حمایت می‌کند.

آموزش تخصصی

در زمینهٔ آموزش مستمر و تخصصی پرسنل پلیسی و قضایی، تلاش‌های قابل ملاحظه‌ای لازم است. تکنیک‌های ارتکاب جرائم مرتبط با رایانه و قابلیت‌های آن با سرعت بیشتری از تکنیک‌های جرائم سنتی تغییر می‌یابند.

برخی از کشورهای عضو اتحادیهٔ اروپا سرگرم اجرای اقداماتی برای آموزش پیشرفتهٔ کارکنان مراکز انتظامی مجری قانون بوده و می‌توانند به کشورهای عضوی که هنوز به چنین قداماتی مبادرت ننموده‌اند، توصیه و رهنمودهایی ارائه دهند.

پروژه‌های شخصی برای رسیدن به این منظور، شکل تبادل تجارب و تشکیل سمینار در مورد چالش‌های مشترکی که با گروه‌های حرفه‌ای ذی‌نفع پیدا می‌کنند، به خود گرفته و با کمک برنامه‌هایی که توسط کمیسیون اداره می‌شوند (به‌ویژه برنامه‌های ایست، شاهین و گرویتوس) به اجرا درآمده‌اند. کمیسیون، طرح فعالیت‌های بیشتری در این زمینه را ادامه خواهد :اد که شامل آموزش‌های رایانه‌ای و اینترنتی هستند.

یوروپول نیز میزبانی دورهٔ آموزشی یک هفته‌ای برای پرسنل مراکز انتظامی کشورهای عضو تحادیه را در نوامبر سال ۲۰۰۰، به‌ویژه با رجوع به مباحث مربوط به هرزه‌نگاری کودکان،

پیشگیری از تحقق جرائم را بیشتر نموده و همچنین اعتماد کاربران به جامعهٔ اطلاعاتی را افزوده است.

واحدهای تخصص‌یافته در سطح ملی

با توجه به پیچیدگی حقوقی و فنی برخی از جرائم مرتبط با رایانه، تأسیس واحدهای تخصصی در سطح ملی، ضروری است. چنین واحدهای تخصصی که متشکل از پرسنلی آگاه با چند تخصص (انتظامی و قضایی) هستند را باید با امکانات فنی کافی تجهیز نمود، تا بتوانند برای تحقق اهداف پیش‌بینی‌شده به‌عنوان نقاط ارتباطی سریع وارد عمل شوند. این اهداف عبارتند از:

۱. پاسخگویی سریع به درخواست اطلاعات در مورد جرائم مشکوک. یک قالب مشترک و واحد برای تبادل چنین اطلاعاتی باید مشخص باشد، اگرچه بحث‌های متخصصان کشورهای گروه ۸ نشان داده که این کار با توجه به وجود تفاوت‌هایی در فرهنگ‌های حقوقی داخلی کشورها آسان نیست.

۲. اقدام تحت عنوان یک مجری رابط در سطح داخلی و بین‌المللی برای تلفن‌هایی که جهت ابراز شکایت از نشر مطالب غیرمجاز توسط کاربران اینترنت، صورت می‌گیرند.

۳. بهسازی و توسعهٔ تکنیک‌های ویژهٔ تعقیب رایانه‌ای به‌منظور کشف، رسیدگی و تعقیب جرائم مرتبط با رایانه.

۴. وجود مراکزی به‌عنوان یک مرکز ممتاز در مورد مباحث مربوط به جرائم اینترنتی به‌منظور ارائه و تبادل بهترین تجارب و راهکارها.

برخی از کشورهای عضو اتحادیهٔ اروپا، چندی است این واحدهای تخصصی را که منحصراً متولی رسیدگی به جرائم مرتبط با رایانه هستند، تأسیس کرده‌اند. عقیده کمیسیون بر این است که احداث چنین واحدهایی حق قانونی هر یک از کشورهای عضو اتحادیه بوده و آنها را به انجام اقداماتی در این راستا ترغیب می‌کند. خرید و نصب جدیدترین نرم‌افزارها و

ـ تقویت همکاری بین مراکز انتظامی مجری قانون، بخش صنعت، سازمان‌های مربوط به مصرف‌کننده (کاربر) و مراجع حفاظت اطلاعات؛

ـ ترغیب صنایع مرتبط و راهکارهای متناسب که از سوی بخش صنعت و مجمع به‌طور مشترک اداره می‌شوند، از قبیل اقداماتی در حمایت از محصولات امنیتی.

موضوع رمزنگاری نیز احتمالاً در این زمینه همچنان حائز اهمیت خواهد بود. رمزنگاری ابزاری مهم برای تسهیل اجرا و به‌کارگیری خدمات جدید، شامل تجارت الکترونیکی است و می‌تواند به جلوگیری از تحقق جرائم در اینترنت کمک شایانی نماید. خط‌مشی کمیسیون در مورد رمزنگاری در بیانیه ۱۹۹۷ آن در خصوص اعتماد و اطمینان در ارتباطات الکترونیکی مطرح شده و طی آن کمیسیون ابراز می‌دارد که تمام محدودیت‌های موجود بر گردش آزاد محصولات رمزگشا را در سطح جامعهٔ اروپایی لغو خواهد کرد. این بیانیه، همچنین اعلام می‌دارد که محدودیت‌های داخلی هر کشور بر گردش آزاد محصولات رمزنگاری باید همسو با قوانین جمعی اروپا باشند. کمیسیون، عقلانی بودن چنین محدودیت‌هایی را در سطح داخلی، به‌ویژه با توجه به موازین مربوط به گردش آزاد محصولات در معاهدهٔ اروپا، رویهٔ قضایی دادگستری و شروط دستورالعمل‌های حفاظت اطلاعات، بررسی خواهد کرد. در عین حال، کمیسیون واقف است که رمزنگاری، به‌وجود آورنده چالش‌های دشوار و جدیدی برای مراکز انتظامی مجری قانون نیز می‌باشد.

بنابراین، کمیسیون از مقرراتی که (اخیراً) در خصوص کالاهای دومنظوره، بازنگری و تصویب شده‌اند و همچنین تا حدود زیادی محدودیت دسترسی به محصولات رمزنگاری را برمی‌دارند، استقبال کرده و در عین حال به ضرورت همراهی این مقررات با مذاکرات مناسب‌تری میان کاربران، بخش صنعت و مراکز انتظامی واقف نمی‌باشد. کمیسیون به نوبهٔ خود قصد دارد از طریق طرح گردهمایی اتحادیهٔ اروپا، این گفت‌وگوها را در سطح اتحادیه ارتقا بخشد. فراهم بودن گستردهٔ محصولات رمزنگاری در سطح اتحادیهٔ اروپا، شامل محصولات پیشرفتهٔ رمزنگاری که در صورت لزوم با معیارهای توافقی ارزیابی هم سنجیده می‌شوند، امکان

ارزش استنادی داده‌های رایانه‌ای

حتی در مواردی که مراجع انتظامی مجری قانون به اطلاعات رایانه‌ای که ادلهٔ قانونی به‌نظر می‌رسند دست یافته باشند، باید بتوانند این اطلاعات را برای استفاده در پی‌جویی و پیگرد جرائم، بازیابی و تصدیق کنند. با توجه به ماهیت و سهولت تخدیش، تحریف یا حذف اطلاعات الکترونیکی و عبور از موارد امنیتی فنی، این کار به‌سادگی انجام‌پذیر نیست. علوم جنایی رایانه‌ای، توسعه و به‌کارگیری پروتکل‌های علمی و شیوه‌های تفتیش رایانه‌ها و تجزیه و تحلیل و حفظ صحت اطلاعات بازیافت شده را عهده‌دار گشته است.

به تقاضای متخصصان کشورهای گروه ۸ ، سازمان بین‌المللی ادلهٔ رایانه‌ای (IOCE) موافقت کرده تا دستورالعمل‌هایی را برای تدوین استانداردها، شامل تعریف اصطلاحات مشترک، روش‌های تشخیص هویت، تکنیک‌های مورد استفاده و ایجاد یک قالب مشترک برای درخواست‌های جنایی ارائه دهد. اتحادیه اروپا نیز باید در این امر، هم از طریق واحدهای پی‌جویی تخصصی کشورهای عضو برای جرائم اینترنتی و هم از طریق R&D که مورد حمایت برنامهٔ اساسی پنجم است (برنامهٔ IST)، مشارکت نماید.

اقدامات غیرتقنینی

قانونگذاری مناسب در سطح داخلی و بین‌المللی، لازم اما به تنهایی برای مبارزه با جرائم مرتبط با رایانه و سوءاستفاده از شبکه کافی نیست. شماری از اقدامات مکمل و غیرتقنینی برای تکمیل اقدامات قانونگذاری لازم است.

اکثر این اقدامات غیرتقنینی در دستورالعمل‌های مطالعهٔ COMCRIME که کشورهای گروه ۸ در طرح اجرایی ۱۰ مرحله‌ای خود ارائه کرده‌اند، مطرح شده و رایزنی‌های غیررسمی بسیاری پیش از تدوین این گفتار در حمایت از آن انجام شده است. از جمله این اقدامات عبارتند از؛

ـ ایجاد واحدهای تخصصی پلیس برای مبارزه با جرائم رایانه‌ای در سطح داخلی در نقاطی از این واحدها که تاکنون وجود نداشته‌اند؛

شناسایی صلاحیت کشورها جهت پی‌جویی جرائم وجود داشته باشد، به طوری‌که تمام کشورها از صلاحیت محلی برخوردار گردند. اصول عمده‌ای که در پیش‌نویس کنوانسیون شورای اروپا مطرح شده‌اند، عبارتند از؛ صلاحیت توسط کشوری احراز شود که جرم در حوزهٔ آن یا توسط تبعهٔ آن رخ داده است. وقتی بیش از یک کشور مدعی صلاحیت باشد، کشورهای درگیر باید با نظری در راستای تعیین صلاحیت متناسب به مشورت بپردازند. البته، بخش بزرگی از کار به شور مؤثر دو یا چند جانبهٔ طرفین بستگی دارد. کمیسیون همچنان این موضوع را جهت تشخیص لزوم انجام اقدامات بیشتری در سطح اتحادیهٔ اروپایی مورد بازنگری قرار خواهد داد.

کمیسیون که در گفت‌وگوهای شورای اروپا و کشورهای گروه ۸ شرکت نموده، به پیچیدگی و معضلات مربوط به مباحث قوانین آیین دادرسی پی برده است. اما به هر حال، همکاری بین کشورهای عضو اتحادیهٔ اروپا در مبارزه با جرائم اینترنتی، عامل اساسی در ایجاد یک جامعهٔ اطلاعاتی امن‌تر و حوزه‌ای از آزادی، امنیت و عدالت است. کمیسیون همچنان قصد دارد با هدف کار بر روی این موضوع به رایزنی‌های خود با گروه‌های دخیل، طی ماه‌های آینده ادامه دهد. این مبحث همچنین در بستری وسیع‌تر، اقدامات کمیسیون در جهت اجرای نتایج شورای اروپا در تامپر در اکتبر ۱۹۹۹ را مد نظر قرار خواهد داد. به‌خصوص شورای تامپر از کمیسیون اروپایی خواست تا دسامبر سال ۲۰۰۰، طرحی در جهت به اجرا درآوردن اصل شناسایی متقابل در تصمیمات قضایی را مورد پذیرش قرار دهد. کمیسیون چندی پیش مقاله‌ای در مورد شناسایی متقابل تصمیمات نهایی در مورد موضوعات جنایی منتشر کرده است.

کمیسیون به‌عنوان بخشی از تلاش خود جهت اجرای قسمتی از طرح اجرایی مربوط به دستورالعمل‌های پیش از دادرسی، به طریق زیر اقدام می‌کند: کمیسیون، گزینه‌هایی برای شناسایی متقابل دستورالعمل‌های پیش از دادرسی مرتبط با پی‌جویی‌های جرائم اینترنتی را با هدف ارائه یک طرح قانونگذاری براساس بند پنجم از معاهدهٔ اتحادیهٔ اروپا، بررسی خواهد کرد.

است، مسائل بسیار پیچیده‌تر می‌گردد. در این شرایط، موارد مهمی چون حاکمیت، حقوق‌بشر و مراکز انتظامی مجری قانون دخیل‌اند که باید بین آنها توازن برقرار شود.

ابزارهای حقوقی موجود برای همکاری بین‌المللی در موضوعات حقوق کیفری، از قبیل همکاری حقوقی دوجانبه، ممکن است ناکافی یا نامناسب باشند، چراکه اجرای آنها اغلب روزها، هفته‌ها یا حتی ماه‌ها به طول می‌انجامد. بنابراین نیاز به سازوکاری است که به‌واسطهٔ آن کشورها بتوانند به پی‌جویی جرائم پرداخته و به سرعت و به‌صورت کارآمد، ادلهٔ لازم را به‌دست آورده، یا حداقل ادله و شواهد مهم به‌دست آمده توسط مجریان قانون فرامرزی را به‌دست آورند و این کار را همسو با اصول حاکمیت ملی، حقوق اساسی و حقوق بشر، از قبیل حفظ حریم خصوصی و حفاظت اطلاعات انجام دهند.

طرح‌های پیشنهادی جدید که در پیش‌نویس کنوانسیون شورای اروپا برای مقابله با جرائم اینترنتی و مشکلات ناشی از آنها ارائه و در دست بررسی هستند، شامل دستوراتی برای حفظ اطلاعات به‌منظور پیشبرد موارد تعقیب ویژه هستند. در هر حال دیگر مباحث، مانند جست‌وجو و توقیف برون مرزی، مسائلی دشوار و حل‌نشده در سیاستگذاری پیش می‌آورند. برای مواجهه با هرگونه ابتکار واقعی، بحث و گفت‌وگوی بیشتری بین احزاب دخیل لازم است.

اعضای کشورهای گروه ۸ ، در مورد جرائم مربوط به فناوری پیشرفته، موضوع تفتیش و توقیف برون‌مرزی را به بحث گذاشته و با در نظر گرفتن توافقی پایدار در آینده، به اتفاق‌نظر در مورد اصول موقت دست یافته‌اند. اما، پرسش‌های مهم دیگری نیز مانند اطلاع از زمان، امکان تفتیش و توقیف در موقعیت‌های ویژه پیش از باخبر کردن کشور مورد جست‌وجو و احتیاج به ساخت حفاظ‌های متناسب برای رعایت حقوق بنیادی، باید مطرح شوند. در موضع مشترک اتحادیهٔ اروپا در خصوص پیش‌نویس کنوانسیون شورای اروپا پیرامون جرائم اینترنتی، وزرا موضعی بی‌حاصل اتخاذ کرده‌اند. [بدون نتیجهٔ نهایی]

در موارد مربوط به جرائم اینترنتی فرامرزی، لازم است قوانین روشنی در خصوص

عملکرد این حوزه، طرح‌های شورا هر چه سریع‌تر باید به اجرا رسند، البته موفقیت این شبکه مستلزم به‌کارگیری کارکنانی است که هم به لحاظ فنی و هم به لحاظ حقوقی، تخصص و مهارت لازم را داشته باشند که این امر به معنای ارائه آموزش‌های متناسب است.

نیازی مشابه برای افزایش همکاری و تبادل اطلاعات بین مسئولان مراکز گمرک نیز وجود دارد. اشکال موجود برای همکاری را باید توسعه داد و راهکارهای جدیدی برای اجرای عملیات‌های مشترک و تبادل اطلاعات به‌وجود آورد. با توجه به درخواست حفاظت از اطلاعات، ضروری است توافقی فراگیر بین مراکز گمرک و شبکه‌های بین‌المللی اطلاعات برای تسهیل و تسریع فرآیند تبادل اطلاعات، به‌وجود آید. همچنین، لزوم سرمایه‌گذاری بیشتری نیز در این زمینه مشهود می‌باشد. مجهز شدن به سیستم‌های رایانه‌ای و همچنین آموزش پرسنل گمرک برای افزایش کارآیی وظایف مراکز گمرک از این قبیل سرمایه‌گذاری‌ها به‌شمار می‌آید.

توانایی و صلاحیت قوانین آیین دادرسی

در سطح داخلی، در صورت احراز شرایط خاص قانونی، مجریان قانون باید قادر باشند تا به سرعت داده‌های ذخیره شده در رایانه‌ها را جست‌وجو و ضبط کنند تا از نابودی ادلهٔ کیفری جلوگیری به‌عمل آید. مقامات مجری قانون معتقدند که آنها باید از اختیارات کافی در حوزهٔ صلاحیت خود به‌منظور تفتیش سیستم‌های رایانه‌ای، ضبط اطلاعات و صدور دستور به افراد برای تحویل داده‌های خاص رایانه‌ای و صدور دستور تحصیل، برداشت یا ذخیرهٔ فوری، داده‌های خاصی را بر طبق قواعد دادرسی و ضوابط حقوقی مرسوم، داشته باشند، اما در حال حاضر این ضوابط و قواعد دادرسی همسان شده نیستند.

اگر هنگام استفاده از یک رایانه، مراکز مجری قانون دریابند که در این دسترسی شماری از رایانه‌ها و شبکه‌ها در سراسر کشور درگیرند، ممکن است سؤالاتی پیش آید. اگر در هنگام تفتیش یک رایانه یا پی‌جویی جرمی از سوی مراکز مجری قانون، متوجه شوند که این کار به دسترسی یا لزوم دسترسی به اطلاعاتی که در یک یا بیش از یک کشور دیگر قرار دارند نیاز

قاچاق مورد استفاده قرار می‌گیرد، ابزاری باارزش و کارآمد است.

از سوی دیگر این عملیات، مشکلات عملی و حقوقی عمده‌ای را برای مراجع قضایی و انتظامی مجری قانون در زمان انجام کار به‌وجود آورده، که از آن جمله فراهم آوردن ادله فرامرزی با Commission Rogatoire شناسایی قربانیان و نقش سازمان‌های بین‌المللی دولتی که با موازین پلیسی سر و کار دارند (اینترپول و به‌خصوص یوروپول) است.

به‌منظور داشتن همکاری مفید بین‌المللی، شبکه‌های ارتباطی بین‌المللی برای مبادلهٔ اطلاعات بیش از پیش برای پلیس و مأموران گمرک اهمیت می‌یابند. مدتی است که بین کشورهای گروه ۸، یک شبکه اطلاعاتی ۲۴ ساعته در هفت روز هفته برای ارتباط مراجع انتظامی مجری قانون، تأسیس و راه‌اندازی شده است. هدف اصلی از ایجاد این شبکه، دریافت و پاسخ‌گویی به تقاضاهای فوری برای همیاری در به‌دست آوردن ادلهٔ الکترونیکی[1] است. این شبکه در چندین مورد با موفقیت مورد استفاده قرار گرفته است. شورای اروپا در JHA در ۱۹ مارس ۱۹۹۸، ۱۰ اصل برای مبارزه با جرائم مربوط به فناوری پیشرفته را به تصویب رسانید که توسط کشورهای گروه ۸ تأیید و به کار گرفته شده است. این شورا از کشورهای غیر گروه ۸ عضو اتحادیه نیز خواسته است تا به این شبکه بپیوندند. این نقاط ارتباط باید مستقیماً با یکدیگر همکاری کرده و ابزار موجود برای همکاری متقابل و کانال‌های ارتباطی را ایجاد نمایند.

ایجاد چنین شبکه‌ای در پیش‌نویس کنوانسیون شورای اروپا نیز پیش‌بینی شده است. که شامل موارد زیر است: ارجاع به نقاط ارتباط شبکه ۲۴ ساعته، تصمیمات در خصوص مبارزه با هرزه‌نگاری کودکان در اینترنت، موضع مشترک اتحادیه اروپا در پیش‌نویس کنوانسیون شورای اروپا پیرامون جرائم اینترنتی، تصمیم شورا در تأیید طرح اجرایی کشورهای گروه ۸، اما هیچ‌گونه اقدام خاصی از سوی اتحادیهٔ اروپا در این زمینه صورت نگرفته است.

کمیسیون بر این باور است که با توجه به نیاز مبرم به خبرگی متناسب و سرعت در

---

1. Electronic Reasons

در بیانیهٔ نهایی کنفرانس وزرا در بن، ۶ تا ۸ جولای ۱۹۹۷، در مورد شبکه‌های اطلاعاتی جهانی اعلام کردند که اصل بر این است که چون یک کاربر حق حضور بی‌نام در محیط غیرشبکه‌ای را دارد، در محیط مجازی اینترنت هم این حق انتخاب باید برای او محفوظ بماند. بنابراین، توافقی آشکار در خصوص لزوم بررسی فعالیت‌های رایج بر روی شبکه با استفاده از اصول بنیادین حقوقی که در سایر نقاط نیز اعمال می‌شوند، وجود دارد. اینترنت یک حلبی‌آباد آشوب‌زده نیست که در آن مقررات اجتماع قابل اعمال نباشند. به همین نسبت، اختیارات دولت و مراجع عمومی در محدود کردن حقوق افراد و کنترل رفتارهای غیرقانونی در شبکه‌های ارتباطی عمومی، نباید بیش از اختیارات آنها در دنیای واقعی غیراینترنتی، باشد. این خواسته همان‌طور که باید در مورد اعمال محدودیت بر حقوق بنیادین و آزادی‌های فردی به خوبی توجیه شده و متناسب با دیگر اهداف سیاست عمومی می‌باشد، باید در محیط مجازی اینترنت نیز لحاظ شود.

در ماده ۲۹ از بیانیهٔ حزب کارگری در مورد حفاظت اطلاعات، به تفصیل چگونگی تحقق این هدف (مثلاً در خصوص پست الکترونیک، گروه‌های خبری[1] و غیره) بیان شده است. کمیسیون اروپا هم با نقطه‌نظرات بیان‌شده از سوی حزب کارگری موافق می‌باشد.

همکاری مفید در سطح بین‌المللی

در سال‌های اخیر، مراکز انتظامی مجری قانون در سطح جهانی به عملیات متحدالشکل، از قبیل عملیات استاربورست و کدرال[2] علیه گروه‌های سوءاستفاده کننده جنسی از کودکان دست زده‌اند که این مسئله نشانگر اهمیت اقدامات مشترک بین‌المللی توسط مراجع انتظامی و قضایی، هم در تبادل اطلاعات در مراحل اولیه و هم در جلوگیری از رسیدن اطلاعات محرمانه به دیگر اعضای گروه‌ها پس از دستگیری و توقیف است. اینترنت در تحقیقات پلیس و مأموران گمرک، به‌خصوص در حالیکه به‌عنوان ابزاری برای ارتکاب جرائم سنتی مانند جعل و

---

1. Usenet
2. Cathedral

متغیر که در آن آدرس‌ها تنها برای یک دوره کوتاه و نه بر مبنای ثابت به کاربران اعطا می‌گردد، فراهم آورده می‌شود.

برخی از نمایندگان بخش صنعت در مذاکرات خود با کمیسیون اروپا، به‌علت حفظ امنیت خود در برابر کلاهبرداری و از دست رفتن انسجام شبکه، خواستار اختفای کامل نبودند. بورس اینترنت لندن بهترین رهنمودهای کاربردی که خود به کار بسته و در انگلستان مفید واقع شده را اعلام کرده است. اما دیگر نمایندگان بخش صنعت و متخصصان حافظ حریم خصوصی بیان کرده‌اند که در صورت عدم اختفای هویت، نمی‌توان رعایت حقوق بنیادین فردی را تضمین کرد.

بند ۲۹ از بیانیهٔ حزب کارگری در خصوص حفاظت اطلاعات، دستورالعملی برای نحوه استفادهٔ بی‌نام و نشان از اینترنت صادر کرده است. این بند، موضوع اختفای هویت در اینترنت را محور یک تنگنا برای دولت‌ها و سازمان‌های بین‌المللی محسوب می‌کند. چراکه، از یک سو برای رعایت حقوق بنیادین فرد نسبت به حریم خصوصی، آزادی بیان و حفظ آنها در محیط مجازی اینترنت، امکان اختفای هویت ضروری است و از سوی دیگر، توانایی داشتن ارتباط اینترنتی و شرکت در آن بدون فاش شدن هویت شخص، برخلاف اقدامات اساسی برای حمایت از دیگر حوزه‌های کلیدی موازین عمومی مانند؛ مبارزه علیه انتشار مطالب غیرقانونی و زیان‌آور، کلاهبرداری مالی و نقض حقوق مؤلف، صورت می‌گیرد. البته این تضاد آشکار بین اهداف مختلف موازین عمومی امر جدیدی نیست.

در مورد روش‌های قدیمی‌تر ارتباط غیراینترنتی، مانند ارسال نامه و بسته، تلفن، روزنامه‌ها، یا پخش از طریق رادیو و تلویزیون، توازنی بین این اهداف برقرار شده است. چالشی که اینک پیش‌روی سیاستگذاران موازین عمومی قرار دارد، عبارت از حصول اطمینان از رعایت حقوق بنیادین اشخاص و در عین حال اعمال محدودیت‌های متناسب در مواقع خاص بر این حقوق، در بستر محیط مجازی اینترنت است. میزان و محدودیت توانایی یک شخص، برای حضور در اینترنت به روش بی‌نام و نشان، نقشی کلیدی در این توازن دارد.

پرهزینه هستند، رودررو کرد. به‌منظور جلوگیری از افزایش هزینه و کاهش قابلیت دسترسی به اینترنت برای کاربران، باید در به‌کارگیری هرگونه ابزاری علیه جرائم اینترنتی، اثرات اقتصادی آن‌را با کارآمدی‌اش قیاس کرد. امنیت کافی برای حفاظت اطلاعات مبادله‌شده باید تضمین گردد.

در هر حال، بخش صنعت نقشی کلیدی در فرآیند ایجاد یک جامعهٔ اطلاعاتی امن‌تر ایفا می‌کند. کاربران باید به امنیت جامعهٔ اطلاعاتی اطمینان داشته و نسبت به عدم بروز جرائم و نقض حریم خصوصی خود، آسوده‌خاطر باشند.

کمیسیون با جدیت از گفت‌وگویی سازنده میان مراجع انتظامی، بخش صنعت، مراجع حفاظت اطلاعات داده‌ها و سازمان‌های مصرف‌کننده (کاربران) و دیگر گروه‌های ذی‌نفع حمایت می‌کند. در چارچوب گردهمایی پیشنهادی اتحادیه اروپا (به بخش ۶۰۴ از این گفتار رجوع کنید.)، کمیسیون از تمام گروه‌های ذی‌نفع می‌خواهد تا به‌عنوان یک اولویت، موضوع پیچیدهٔ حفظ و نگهداری داده‌های مبادله‌شده را به‌طور مفصل به بحث گذاشته و به‌طور مشترک برای یافتن راهکارهای مناسب، متوازن و متناسب که حقوق بنیادین فرد نسبت به حریم خصوصی خود و مراقبت از داده‌ها را محترم شمارد، اقدام نمایند. بر مبنای دستاورد این تلاش کمیسیون قادر خواهد بود نیاز به هرگونه اقدام قانونگذاری یا غیرتقنینی در سطح اتحادیه اروپا را ارزیابی کند.

دستیابی و استفادهٔ بی‌نام و نشان

متخصصان علوم انتظامی نسبت به امکان بی‌نام بودن کاربران و عدم انتساب مسئولیت به آنها و عدم امکان به دام انداختن برخی از مجرمان خاص، ابراز نگرانی کرده‌اند. استفادهٔ بی‌نام از ارتباط تلفنی موبایل در برخی از کشورها از طریق کارت‌های پیش‌پرداختی میسر است. دسترسی بی‌نام به اینترنت توسط برخی تأمین‌کنندگان خدمات، از قبیل مراکز ارسال پیام و کافی‌نت‌های اینترنتی، میسر شده است. اختفای هویت تا اندازه‌ای به‌وسیلهٔ سیستم آدرس‌دهی

نگهداری شدید از اطلاعات شخصی، موضع مشخصی را اتخاذ کرده است.

در هر حال، در مذاکرات پیرامون مقابله با هرزه‌نگاری کودکان در اینترنت، این پارلمان طی ۳ ماه عقیده‌ای مبنی بر ضرورت یک الزام عمومی در حفظ تبادل اطلاعات را ابراز نموده و بر آن پافشاری کرده است.

این امر مبین اهمیت بستری است که در آن موضوع حساسی، مانند حفاظت از تبادل اطلاعات به بحث گذاشته می‌شود و نیز نشانگر چالشی است که گریبانگیر سیاستگذارانی که سعی در ایجاد موازنه‌های مناسب دارند، می‌باشد.

کمیسیون بر این باور است که هرگونه راهکاری در خصوص مبحث پیچیدهٔ حفاظت تبادل اطلاعات باید به خوبی تبیین شده، متناسب بوده و موازنه‌ای عادلانه و درست بین منافع گوناگون در این چارچوب به‌وجود آورد. منحصراً رهیافتی که موجب نزدیکی و ایجاد توازن میان مهارت و توانایی‌های دولت، صنعت و مراجع ناظر بر حفاظت اطلاعات و کاربران شود و بتواند در تحقق این هدف مؤثر باشد. اتخاذ یک رویکرد همسان میان کشورهای عضو اتحادیه اروپا در این مقوله دشوار، بسیار مطلوب خواهد بود. چنین رویکردی، اهدافی چون کارآمدی، تناسب و پرهیز از وضعیتی که در آن هم مراجع انتظامی و هم جامعهٔ کاربران اینترنت به‌ناچار با آشفته بازاری از محیط‌های فنی و حقوقی گوناگون درگیر شوند را تعقیب می‌نماید. بنابراین، مسائلی مهم و کاملاً متفاوت از یکدیگر را باید در نظر گرفت. از یک‌سو، مراجع ناظر بر حفاظت اطلاعات بر این باورند که کارآمدترین ابزار برای کاستن از خطرات نقض حریم خصوصی در هنگام تشخیص موارد موردنیاز مراجع انتظامی این است که نباید اطلاعات مبادله‌شده را منحصراً به‌منظور استفادهٔ مراجع انتظامی نگاه داشت. از سوی دیگر، مراجع انتظامی پیگیر جرائم بیان کرده‌اند که نگهداری حداقل اطلاعات در کمترین زمان ممکن برای پیشبرد تحقیقات کیفری ضروری است.

بخش صنعت نیز به مشارکت در مبارزه علیه جرائمی مانند نفوذ به سیستم‌های رایانه‌ای (Hacking) و اختلاس رایانه‌ای متمایل است، اما نباید این بخش را با ابزارهایی که بی‌دلیل

برای ارتباطات راه دور با نرخ ثابت یا رایگان، تأمین‌کنندگان خدمات اساساً مجاز بـه حفـظ اطلاعات مبادله‌شده‌ای هستند که براساس دستورالعمل‌هـای اتحادیـه اروپـا در مـورد حفاظـت داده‌ها معین می‌شوند و کشورهای عضو اتحادیه می‌توانند برای محدود ساختن دامنـه الزامـات جهت پاک کردن اطلاعات مبادله شده از ابزارهای قانونگذاری استفاده نمایند. یعنی هنگامی‌کـه این داده‌ها بخشی از ابزارهای لازم برای جلوگیری، تحقیق، پی‌جویی جرائم یا استفاده غیرمجاز از سیستم‌های ارتباط راه دور باشند. البته، هرگونه اقدام برای قانونگذاری در سطح داخلـی کـه نگهداری اطلاعات مبادله‌شده برای اهداف تحقیقاتی را مجـاز شـمارد بایـد شـروط خاصـی را دربرداشته باشد؛ اقدامات (قوانین) مفروض باید، به‌موقع، موردنیاز و متناسب باشند.

ایـن شـروط از جملـه الزامـات قـوانین جمعـی و قـوانین بـین‌المللـی اسـت کـه شـامل؛ دستورالعمل‌های ۹۷/۶۶ (EC) و ۹۵/۴۶ EC، کنوانسیون اروپایی ۴ نوامبر ۱۹۵۰ در خـصوص رعایت حقوق‌بشر و کنوانسیون شـورای اروپـا بـرای حفاظـت از شـخص در برابـر پـردازش خودکار داده‌های شخصی که در ۲۸ ژانویه ۱۹۸۱ به تصویب رسیده است، می‌باشد.

این امر به‌ویژه برای اقـداماتی (قـوانینی) کـه رونـد معمـول در نگهـداری و ذخیـره‌سـازی اطلاعات توسط بخش عظیمی از کاربران را دربرمی‌گیرند، حائز اهمیت است.

برخی از کشورهای عضو اتحادیه درصدد تدوین موازین حقوقی هستند که تـأمین‌کننـدگان خدمات اینترنت را مجاز یا ملزم می‌سازد که پس از ارائه خدمت، بخـش خاصـی از اطلاعـات مبادله‌شده را که جهت ارسال صورت‌حساب موردنیاز نبوده، امـا در پیـشبرد تحقیقـات جنـایی مفید محسوب می‌شوند را نگاه دارند.

دایره شمول و شکل این موازین تفاوت بسیاری داشته، اما همگی بر این ایده اسـتوارند کـه اطلاعات بیش از آن‌که تأمین‌کنندگان خدمات صرفاً برای ارائه خدمت خـودپردازش نگهـداری می‌کنند باید برای مراجع انتظامی پیگیـر جـرائم در دسـترس باشـد. کمیـسیون اروپـا در حـال ارزیابی این ابزارهای حقوقی در راستای قوانین موجود اتحادیه است.

پارلمان اروپا به مباحث مربوط بـه حـریم خـصوصی حـساس بـوده و عمومـاً در راسـتای

عموماً در صلاحیت اعضای اتحادیه و بند پنجم از معاهده اتحادیه اروپا هستند، با الزامات قوانین جمعی اطمینان حاصل می‌شود.

به‌ویژه دادگاه کیفری همواره تأکید داشته که چنین اصول حقوقی نباید علیه اشخاصی که براساس قوانین جمعی، حق برخورد برابر را دارند، تبعیض روا داشته یا آزادی‌های مشروعی را که برای آنها تضمین شده، محدود نماید. هرگونه قوای جدید برای مراجع انتظامی باید در قیاس با قوانین جمعی و تأثیر آنها بر حریم خصوصی، ارزیابی شوند.

حفاظت از اطلاعات مبادله‌شده

مراجع انتظامی اغلب برای انجام تحقیقات و پی‌جویی جرائمی که با استفاده از شبکه‌های ارتباطی و اینترنت، صورت می‌گیرند، از اطلاعات حاصل از تبادل اطلاعات که به‌منظور تنظیم صورتحساب مشتریان توسط تأمین‌کنندگان خدمات اینترنتی ذخیره می‌شوند، استفاده می‌کنند.

از آنجا که نرخ درخواستی برای خدمات ارتباطی کمتر از گذشته به فاصله و مقصد ارتباطی وابسته است و تأمین‌کنندگان خدمات هم به نرخ‌گذاری یکنواخت و ثابت روی می‌آورند، دیگر نیازی به ذخیره‌سازی اطلاعات مبادله‌شده برای تنظیم و ارسال صورت‌حساب نیست.

بدین ترتیب، مراجع انتظامی از آن بیمناک هستند که این امر موجب کاهش مطالب مفید و مورد استفاده در کار تحقیقات شود؛ بنابراین به تأمین‌کنندگان خدمات توصیه می‌کنند که مقدار مشخصی از اطلاعات مبادله‌شده را حداقل برای کمترین زمان ممکن و برای استفاده توسط مراجع انتظامی، ذخیره و نگهداری کنند.

برطبق دستورالعمل‌های اتحادیه اروپا در مورد حفاظت از اطلاعات شخصی، چه براساس اصول کلی و محدود دستورالعمل ۹۵/۴۶ کمیسیون اروپا (EC) و چه اصول اخذ دستورالعمل ۹۷/۶۶ آن کمیسیون، اطلاعات مبادله‌شده باید بلافاصله پس از انجام خدمات ارتباطی پاک یا بی‌نام و نشان شوند، مگر اینکه حفظ آنها برای ارائه صورت‌حساب لازم باشد.

نوع نژادپرستی و بیگانه‌ستیزی اینترنتی و غیراینترنتی را دربرداشته باشد. این طرح از ارزیابی آتی نحوه اجرای عملکرد مشترک ۱۵ جولای ۱۹۹۶ کشورهای عضو علیه نژادپرستی و بیگانه‌ستیزی استظهار خواهد جست. این اقدام مشترک، نخستین اقدامی است که در جهت همسان‌سازی جرائم مربوط به نژادپرستی و بیگانه‌ستیزی قلمداد می‌شود. اما همچنان نیاز بیشتری به همسان‌سازی قوانین در درون اتحادیه اروپا وجود دارد. اهمیت و حساسیت این موضوع با تصمیم یک دادگاه فرانسوی در ۲۰ نوامبر سال ۲۰۰۰ که سایت یاهو را وادار به مسدود کردن دسترسی کاربران فرانسوی به سایت‌هایی که یادگاری‌های نازی‌ها را می‌فروختند، مشخص می‌شود.

و سرانجام کمیسیون چگونگی اصلاح کارآیی اقدامات انجام‌شده علیه تجارت غیرقانونی موادمخدر در اینترنت را بررسی خواهد کرد . اهمیت این موضوع را می‌توان در استراتژی اتحادیه اروپایی در قبال موادمخدر بین سال‌های ۲۰۰۰ تا ۲۰۰۴ که در شورای اروپا در هلسینکی به تأیید رسید، مشاهده کرد.

مشکلات مربوط به قوانین آیین دادرسی

ماهیت جرائم مرتبط با رایانه، مشکلات آیین دادرسی را به صحنهٔ توجهات داخلی و بین‌المللی از قبیل حاکمیت‌ها و قوانین مختلف تبدیل کرده است.

سرعت اجرا، تحرک و انعطاف‌پذیری جرائم رایانه‌ای، بیش از هر جرم فرامرزی دیگری، قوانین آیین دادرسی کیفری موجود را با چالش روبرو می‌کند.

همسان‌سازی قوانین آیینِ دادرسی، وضعیت نگهداری از قربانیان را با تضمین توانمندی لازم مراجع انتظامی برای پیگیری جرائم در درون حوزه استحفاظی خود، بهبود بخشیده و به آنها اطمینان می‌دهد که مراجع مذکور می‌توانند با سرعت و کارآیی به درخواست همکاری از سوی دیگر کشورها پاسخ مثبت دهند.

همچنین لازم است از همسو بودن اقداماتی که بر مبنای قوانین کیفری صورت گرفته و

موجود در اینترنت ۴) جرائم مربوط به نقض کپی رایت و دیگر حقوق مربوط به آن، اقدام اتحادیهٔ اروپا در همسان‌سازی قوانین می‌تواند از کنوانسیون شورای اروپا که تنها حداقل‌های همسان‌سازی بین‌المللی به‌شمار می‌رود پا را فراتر بگذارد. این اتحادیه می‌تواند در مدت زمانی کوتاه و قبل از اجرایی شدن کنوانسیون COE جنبهٔ اجرایی به خود بگیرد و همچنین می‌تواند جرائم رایانه‌ای را به حوزهٔ شمول قوانین اتحادیه آورده و سازوکارهای اجرایی جدیدی در اتحادیه اروپا ارائه نماید.

این کمیسیون به اقدام مؤثر اتحادیه اروپا به‌ویژه علیه هرزه‌نگاری کودکان در اینترنت، اهمیت زیادی می‌دهد و از تصمیم شورا در مقابله با هرزه‌نگاری کودکان بر روی اینترنت استقبال کرده و در عین حال با دیدگاه پارلمان اروپایی که اقدامات بیشتری را در جهت همسان‌سازی قوانین داخلی لازم می‌داند موافقت کرده است. کمیسیون در نظر دارد که در سال جاری طرح پیشنهادی یک چارچوب شامل دستورالعمل‌هایی برای همسان‌سازی قوانین و ضمانت اجراهای موجود در خصوص هرزه‌نگاری کودکان در اینترنت را ارائه نماید. در راستای تصمیمات نشست شورا در تامپر، کمیسیون یک طرح قانونگذاری تحت عنوان بند پنجم از معاهده اتحادیه اروپا را برای همسان‌سازی قوانین در خصوص جرائم مربوط به فناوری پیشرفته، ارائه داد. این طرح بر پیشرفت حاصله در شورای اروپا استوار بوده و به‌طور اخص بر لزوم همسان‌سازی قوانین مربوط به نفوذ در سیستم و حملات توقف ارائه خدمات می‌پردازد. افزون بر این، طرح شامل تعاریف استاندارد و یکسانی برای اعضای اتحادیه اروپا در این زمینه است. این طرح همچنین می‌تواند با تضمین قابل پیگرد بودن موارد جدی جرائمی از قبیل، نفوذ به سیستم و حملات توقف ارائه خدمات با توسل به حداقل کیفر در تمام کشورهای عضو، از پیش‌نویس کنوانسیون شورای اروپا فراتر رود.

علاوه بر این، کمیسیون میدان عمل را در مواجهه با جرائم مربوط به نژادپرستی و بیگانه‌ستیزی در اینترنت خواهد سنجید و در همان حال به ارائه طرحی پیشنهادی برای تصمیم چارچوبی شورا براساس بند پنجم از معاهده اتحادیه اروپا خواهد پرداخت. به‌طوری که هر دو

ابزار قانونگذاری که ممکن است برای مقابله با جرائم مرتبط با رایانه لازم باشد، نیازمند ایجاد توازن صحیح بین این تمایلات اساسی است.

مشکلات مربوط به قوانین ماهوی

همسان‌سازی حقوق ماهوی در حوزهٔ جرائم مربوط به فناوری پیشرفته تأمین‌کننده حداقل سطح حفاظت از قربانیان جرائم اینترنتی (مثلاً قربانیان هرزه‌نگاری کودکان) خواهد بود. این امر مستلزم آن است که یک فعالیت، قبل از آنکه حمایت‌های قانونی دوجانبه بتواند به تحقیقات کیفری مساعدت نماید، در هر دو کشور جرم شناخته شود (شرط عمل متقابل) و این کار برای بخش صنعت نیز شفافیت بیشتری به‌وجود می‌آورد (به‌عنوان مثال، اینکه مطالب غیرمجاز از چه چیزهایی تشکیل شده‌اند؟).

در واقع به‌کارگیری یک راهکار قانونی در اتحادیهٔ اروپا که قوانین ماهوی کیفری در حوزهٔ جرائم رایانه‌ای را به یکدیگر نزدیک و یکسان سازد، متعاقب نشست شورای اروپا در تامپر در اکتبر ۱۹۹۹ در دستور کار این اتحادیه قرار گرفته است. در این نشست، جرائم مربوط به فناوری پیشرفته به فهرست محدودی از حوزه‌هایی که در آنها باید اقداماتی در جهت توافق بر سر تعاریف، جرم‌انگاری‌ها و مجازات‌های مشترک بین کشورها صورت گیرد، اضافه شد. این نکته در دستورالعمل شماره ۷ استراتژی اتحادیهٔ اروپایی برای هزارهٔ جدید در پیشگیری و کنترل جرائم سازمان‌یافته که در مارس ۲۰۰۰ در مجمع JHA به تصویب رسید، مطرح شده است. این دستورالعمل، بخشی از برنامهٔ کاری کمیسیون اروپایی برای سال ۲۰۰۰ محسوب می‌شود.

کمیسیون، عملکرد شورای اروپا را در مورد کنوانسیون جرائم اینترنتی تعقیب کرده است. چهار گروه از خطاهای کیفری در پیش‌نویس کنوانسیون مجمع اروپایی در مورد جرائم اینترنتی ارائه شده‌اند که عبارتند از: ۱) جرائم علیه حریم خصوصی، تمامیت و قابلیت دسترسی به اطلاعات و سیستم‌های رایانه‌ای، ۲) جرائم مرتبط با رایانه ۳) جرائم مربوط به محتوای مطالب

اجرای الزامات مالیاتی نیز باید مورد توجه قرار گیرد. در خصوص گونه‌ای از مبادلات تجاری که طی آن دریافت‌کنندهٔ متصل به اینترنت یک خدمت الکترونیکی در جایی در اتحادیه اروپا قرار دارد، موجب افزایش الزامات مالیاتی در صلاحیت محلی که استفاده از آن خدمات موردنظر بوده، می‌باشد. عدم پیروی از الزامات مالیاتی، مصرف‌کننده را مستوجب ضمانت اجراهای حقوقی (و در مواردی کیفری) می‌کند که ممکن است شامل مسدود کردن حساب‌های بانکی و یا دیگر سرمایه‌های او شود، اگرچه رعایت داوطلبانه این الزامات همواره موردنظر است، اما در نهایت این الزامات باید لازم‌الاجرا شوند.

همکاری بین سازمان‌های مالیاتی، یکی از عناصر کلیدی نایل شدن به این مطلوب است. ارائه امکان حفاظت از مبادله اطلاعات مشروع به مردم به معنای دادن ابزاری مشابه به مجرمان برای حفاظت از مبادلات غیرمشروع خود است. امکانات حافظ امنیت تجارت الکترونیکی ممکن است در کار قاچاق موادمخدر به‌کار گرفته شوند. در این راه باید ارجحیت‌ها را شناسایی و گزینش‌هایی را انجام داد. حفاظت از قربانیان جرائم مرتبط با رایانه مستلزم پرداختن به موضوعاتی چون مسئولیت کیفری، جبران خسارت و پرداخت غرامت که هنگام وقوع جرائم مرتبط با رایانه پیش می‌آیند، نیز می‌باشد. ایجاد اعتماد نه تنها به فناوری مناسب به‌کار رفته بستگی دارد، بلکه به تضمین‌کننده‌های اقتصادی و حقوقی همراه این فناوری‌ها نیز وابسته است. این مسائل را باید با توجه به گسترهٔ جرائم مرتبط با رایانه مورد بررسی قرار داد.

نیاز به ابزارهای حقوقی ماهوی و آیین دادرسی کارآمدی که همسان با سطح جهانی یا حداقل اروپا باشند، احساس می‌شود تا با اتکا به آنها از قربانیان جرائم مرتبط با رایانه حمایت کرده و مرتکبان به این امر را محاکمه نمائیم. در همین حال، ارتباطات شخصی، حریم خصوصی و حفاظت از اطلاعات، دسترسی و انتشار اطلاعات همگی از حقوق مسلم فرد در دموکراسی‌های مدرن تلقی می‌شوند. به همین جهت، قابلیت دسترسی و استفاده از اقدامات پیشگیرانه به‌منظور کاستن از نیاز و روی آوردن به اقدامات اجرایی، مطلوب است. هرگونه

ذخیره‌سازی اطلاعات اشخاص ثالث استفاده می‌شود، در دستورالعمل مربوط به تجارت الکترونیکی مورد اشاره قرار گرفته است.

ـ جرائم اقتصادی، دسترسی غیرمجاز و خرابکاری؛ بسیاری از کشورها قوانینی در مورد جرائم اقتصادی مختص به رایانه تصویب کرده و جرائم جدیدی مربوط به دسترسی غیرمجاز به سیستم‌های رایانه‌ای (مانند نفوذ به سیستم، خرابکاری رایانه‌ای و انتشار ویروس‌ها، جاسوسی رایانه‌ای، کلاهبرداری و اختلاس رایانه‌ای) و اشکال جدید ارتکاب جرائم (مانند دستکاری در رایانه به جای فریب دادن فرد) را تعریف کرده‌اند. در این جرائم، موضوع جرم اغلب غیرقابل لمس است، به‌عنوان مثال، پول در سپرده‌های بانکی یا برنامه‌های رایانه‌ای. در حال حاضر در اتحادیهٔ اروپا راهکار خاصی در مورد این‌گونه فعالیت‌های غیرمشروع وجود ندارد. در مورد پیشگیری نیز، اخیراً مقرراتی دربارهٔ کالاهای دو کاربردی وضع شده که کمک شایانی به آزادی دسترسی به محصولات رمزنگاری نموده‌اند.

ـ جرائم علیه مالکیت معنوی؛ در مورد مراقبت قانونی از برنامه‌ها و پایگاه‌های رایانه‌ای که مستقیماً مربوط به جامعه اطلاعاتی[1] بوده و زمینه اجرای ضمانت‌های اجرایی را فراهم می‌کند، دو دستورالعمل به تصویب رسیده است. موضع مشترکی در مورد طرح پیشنهادی در خصوص کپی رایت و حقوق مربوطه در جامعه اطلاعاتی از سوی شورا اتخاذ شده و انتظار می‌رود تا اوایل سال ۲۰۰۱ به تصویب برسد. بر این اساس، نقض حق تألیف و حقوق مرتبط همچنین استفاده نکردن از ابزارهای فنی که برای حفاظت از این حقوق طراحی شده‌اند، مستوجب مجازات هستند. در مورد جعل و سرقت، کمیسیون اروپا تا پیش از پایان سال ۲۰۰۰، بیانیه‌ای مبنی بر شمول فرآیند مشاوره که با بیانیه سبز ۱۹۹۸ آغاز شده و طرح اجرایی جدیدی را نیز اعلام می‌دارد، ارائه خواهد کرد. با افزایش اهمیت روزافزون تجارت اینترنتی به تدریج شاهد مشاجراتی بر سر نام‌های دامنه مربوطه و سرقت آنها، انبارسازی و Revers Hijacking خواهیم بود و طبیعتاً برای مواجهه با این مشکلات، نیازمند مقررات و آیین دادرسی جدیدی نیز خواهیم بود.

---

1. Information Society

اتحادیه اروپا، اسناد حقوقی چندی وجود دارد، به جز یک مورد اتخاذ تصمیم شورا در مورد هرزه‌نگاری کودکان در اینترنت، هیچ‌گونه سند حقوقی از سوی اتحادیه اروپا که مستقیماً در خصوص جرائم مرتبط با رایانه اتخاذ شده باشد وجود ندارد، اما چند ابزار حقوقی مرتبط، به‌طور غیرمستقیم موجود است.

مهم‌ترین عناوینی که در قانونگذاری ارتباط با جرائم خاص رایانه‌ای در اتحادیهٔ اروپا یا کشورهای عضو آن موردنظر بوده‌اند، عبارتند از:

ـ جرائم تعرض به حریم خصوصی؛ کشورهای مختلفی اقدام به تصویب قوانین کیفری در مورد جمع‌آوری، ذخیره‌سازی، تغییر و تحریف، افشا و نشر غیرمجاز اطلاعات شخصی کرده‌اند. در اتحادیهٔ اروپا دو دستورالعمل در جهت هم‌سو کردن قوانین کشورهای عضو در مورد حفاظت از حریم خصوصی در روند پردازش اطلاعات شخصی وضع گردیده است.

مادهٔ ۲۴ از دستورالعمل ۴۶/۹۵ کمیسیون اروپا به صراحت کشورهای عضو اتحادیه را به پذیرش کلیه معیارهای ممکن و مناسب برای تضمین اجرای کامل این دستورالعمل وامی‌دارد. از جملهٔ اصول این دستورالعمل، تحمیل ضمانت اجرای کیفری علیه نقض‌کنندگان اصول قوانین داخلی است. موضوع حقوق اساسی نسبت به حریم خصوصی و حفاظت از اطلاعات بیشتر در فصل حقوق اساسی اتحادیه اروپا مورد بررسی قرار می‌گیرد.

ـ جرائم مربوط به محتوا؛ نشر هرزه‌نگاری به‌خصوص هرزه‌نگاری کودکان بر روی اینترنت، همچنین انتشار عبارات نژادپرستانه و اطلاعات ترغیب‌کنندهٔ خشونت، این پرسش را مطرح می‌سازد که تا چه حد می‌توان با توسل به قوانین کیفری موجود به مقابله با این اعمال پرداخت. کمیسیون از این عقیده که هرچه خارج از اینترنت غیرقانونی تلقی شود باید در هنگام اتصال به شبکه نیز غیرقانونی باشد، حمایت می‌کند. نویسنده یا تهیه‌کننده مطالب ممکن است از لحاظ کیفری مسئول تلقی شود. شورا برای مقابله با هرزه‌نگاری کودکان در اینترنت دارای یک مصوبه است.

مسئولیت تأمین‌کنندگان خدمات واسطه که از شبکه‌ها و سرورهای آنها برای انتقال و

دیگر دنیا و در هر زمانی را میسر ساخته‌اند. آمار و ارقام موثقی در خصوص ابعاد کامل پدیدهٔ جرم مرتبط با رایانه وجود ندارد. به احتمال زیاد، شمار اخلال‌گرهایی که تاکنون کشف و گزارش شده‌اند، حجم و مقیاس این معضل را کمتر از آنچه هست، نشان می‌دهند.

به‌دلیل آگاهی و تجربیات محدود مجریان و کاربران سیستم‌ها، بسیاری از اخلال‌گری‌ها مشخص نمی‌شوند. علاوه بر این، بسیاری از شرکت‌ها برای جلوگیری از تبلیغات سوء و خطر حملات آتی، از گزارش مواردی درباره جرائم رایانه‌ای خودداری می‌کنند. بسیاری از مراکز پلیس هنوز‌هم آمار و ارقامی در مورد استفاده از رایانه و سیستم‌های ارتباطی دخیل در این نوع جرائم در اختیار ندارند. اما با گسترش استفاده از رایانه و شبکه‌ها، انتظار می‌رود که شمار فعالیت‌های غیرمشروع نیز افزایش یابد. نیازی آشکار برای جمع‌آوری شواهد موثق در خصوص اهمیت جرائم رایانه‌ای وجود دارد.

در این گفتار، جرم رایانه‌ای در وسیع‌ترین معنای خود به‌کار می‌رود، یعنی به‌عنوان جرمی که به‌نحوی شامل استفاده از فناوری اطلاعات می‌شود. اما در مورد اینکه چه کارهایی «جرم مرتبط با رایانه را شکل می‌دهند» نقطه‌نظرات متفاوتی وجود دارد.

مثالی موضوعی از این امر را می‌توان در حوزهٔ گمرک یافت؛ جایی‌که از اینترنت می‌توان به‌عنوان وسیله‌ای برای ارتکاب جرائم متعارفی علیه قوانین گمرک استفاده کرد، جرائمی مانند قاچاق، جعل و غیره. در حالیکه مبارزه با جرائم خاص رایانه‌ای مستلزم به‌روزکردن تعاریف جرم در قوانین کیفری ـ داخلی است، جرائم سنتی که با کمک رایانه‌ها ارتکاب می‌یابند، نیازمند همکاری و ابزارهای دادرسی اصلاح شده می‌باشند.

در ارتکاب تمامی این موارد از در دسترس بودن اطلاعات و شبکه‌های ارتباطاتی بی‌حد و مرز و گردش اطلاعات غیر ملموس، متغیر و فرار بهره گرفته می‌شود. این ویژگی شبکه‌ها، بازنگری معیارهای موجود در خصوص فعالیت‌های غیرمجازی که با استفاده از شبکه‌ها و سیستم‌ها و یا از طریق آنها صورت می‌گیرند را ضروری می‌سازد.

اغلب، قوانینی در خصوص جرائم مرتبط با رایانه وضع شده است. در کشورهای عضو

به‌منظور حصول کارآیی متقابل بین راهکارها از طریق اجماع و توافق در مورد استانداردهای قوانین بین‌المللی را نیز شامل می‌شود.

همچنین لازم است که هرگونه چارچوب مفهومی که در آینده برای امنیت تدوین می‌شود، بخشی لاینفک از ساختار کلی بوده و از همان آغاز فرآیند طراحی به تهدیدات و آسیب‌پذیری‌های موجود بپردازد. این امر در تضاد با رویکردهای سنتی که به اجبار سعی داشته‌اند تا شکاف‌هایی که مورد بهره‌برداری گروه‌های بزهکار بسیار ماهر بوده‌اند را پر کنند، است.

برنامهٔ فناوری‌های جامعهٔ اطلاعاتی اتحادیهٔ اروپا، به‌خصوص در امور مربوط به اطلاعات و امنیت شبکه و دیگر فناوری‌های اعتمادآفرین، چارچوب مبنایی برای گسترش توانایی و فناوری‌های لازم برای درک و رفع چالش‌های مربوط به جرائم رایانه‌ای را فراهم آورده است. این فناوری‌ها، دربرگیرنده ابزارهایی فنی جهت مراقبت از حقوق مسلم فرد نسبت به حریم خصوصی و اطلاعات شخصی خود و دیگر حقوق فردی و مبارزه با جرائم رایانه‌ای است. علاوه بر این در بطن برنامهٔ فناوری‌های جامعهٔ اطلاعاتی (IST)، یک ابتکار در جهت کسب اعتماد و اطمینان به‌کار رفته است.

این ابتکار شبکه‌ای به جلب اعتماد در زیرساخت‌های اطلاعاتی بسیار به هم پیچیده و سیستم‌های محاط شده، کمک می‌نماید. یکی از بخش‌های لاینفک این اقدام همکاری و وفاق بین‌المللی است. برنامهٔ IST روابطی کاری با سازمان‌های DARPA و NSF به‌وجود آورده که با همکاری وزارت امورخارجهٔ آمریکا اقدام به طراحی یک طرح ضربتی مشترک در مورد مراقبت از زیرساخت‌های حیاتی، نموده است.

در نهایت، اجرای وظایف امنیتی به‌خصوص در پیروی از دستورالعمل‌های حفاظت اطلاعات اتحادیهٔ اروپا به افزایش امنیت و سلامت شبکه‌ها و برنامه‌های پردازش داده‌ها کمک می‌کند.

سیستم‌های پیشرفتهٔ ارتباطی و اطلاعاتی انجام فعالیت‌های غیرمشروع از نقطه‌ای به نقطه

چنان مورد مراقبت قرار گیرند که به‌رغم بروز حوادث و حملات حتی با افزایش حجم انتقال اطلاعات، امر انتقال همچنان میسر باشد. همچنین ارتباطات به خدمات مهمی از قبیل، خدماتی که از سوی سرورهای اسامی ارائه می‌شوند و به‌خصوص، به شمار اندکی از سرورهای اسامی ریشه که آدرس‌های موردنیاز در طی مسیر را مشخص می‌کنند، بستگی دارد. هر یک از این اجزاء نیز نیاز به مراقبت مناسبی دارند که بسته به بخش فضای اسمی و موقعیت کاربری که خدمات به وی عرضه می‌شود، متغیر هستند.

فناوری‌های زیرساخت اطلاعات که با هدف ایجاد انعطاف‌پذیری و پاسخگویی بیشتر به خواست‌های مردم به‌وجود آمده‌اند، اغلب با ناکافی بودن تلاش‌های هدفمند در جهت نگهداری و امنیت، بیش از پیش پیچیده شده‌اند. علاوه بر این، چنین پیچیدگی، برنامه‌های نرم‌افزاری به‌هم پیوسته و دقیق را که در مواقعی شامل ضعف‌ها و شکاف‌های مراقبتی هستند دربرمی‌گیرد، به نحوی‌که ممکن است به‌راحتی برای آسیب رساندن مورد بهره‌برداری قرار گیرند. با پیچیده‌ترشدن محیط مجازی رایانه‌ای و بخش‌های مربوط به آن، ممکن است آسیب‌پذیری‌های جدید و غیرقابل پیش‌بینی در آن ظاهر گردد.

سازوکارهای تکنولوژیکی از چندی قبل موجود بوده و موارد جدیدی نیز جهت بهبود مراقبت در محیط مجازی رایانه‌ای در حال گسترش هستند:

ـ نگهداری از اجزای اصلی زیرساخت از طریق توسعهٔ زیرساخت‌های کلیدی ـ عمومی (PKI)، توسعهٔ پروتکل‌های امنیتی.

ـ مراقبت از محیط‌های رایانه‌ای خصوصی و عمومی از طریق توسعه نرم‌افزارهای کیفی، فایروال‌ها، برنامه‌های ضد ویروس، سیستم مدیریت یا اداره حقوق الکترونیکی، رمزنگاری و غیره.

ـ مراقبت از اعتبار کاربران صلاحیت‌دار، استفاده از کارت‌های هوشمند، شناسایی بیومتریک، امضاهای الکترونیکی، فناوری‌های مبتنی بر نقش و وظیفه.

این موارد مستلزم تلاش بیشتر برای توسعهٔ فناوری‌های امنیتی بوده و لزوم همکاری

مراقبت را باید با مجوز و همکاری کاربران و بر طبق نیازهای آنان به‌کار گرفت.

این امر، به‌ویژه زمانی‌که طیف فعالیت‌هایی که با مراجعه افراد به یک منبع، می‌توانـد انجـام شود را در نظر بگیریم، اهمیتی ویژه می‌یابد. آنها انجام کار و بازی، تماشای تلویزیـون و انجـام امور بانکی را از طریق همان وسیله انجام می‌دهند.

فناوری‌های امنیتی چندی وجود دارند و فناوری‌های جدیدی نیز در حال ظهورنـد. مزایـای توسعهٔ منابع باز به لحاظ امنیت روزبه‌روز آشکارتر مـی‌شـود و بنـابراین فعالیـت بـسیاری در خصوص روش‌های رسمی و معیارهای ارزیابی مراقبت و امنیت صورت گرفته اسـت. اسـتفاده از فناوری‌های رمزنگاری و امضاهای الکترونیکی به‌خصوص با رشد، امکان دسترسی بـی‌سـیم به منابع، ضروری به‌نظر می‌رسـند. انـواع گـسترده‌ای از سـازوکارهای تـصدیق صـحت بـرای برآوردن نیازهای ما در محیطی که در آن تعامل داریم، لازم است.

در برخی محیط‌ها، ممکن است خواسته یا به ضرورت، بی‌نام و نشان بمـانیم و در محیطـی دیگر، ممکن است ناگزیر از تأیید ویژگی خاصی بـدون شناسـایی کامـل شـویم. ماننـد اینکـه بزرگسال بودن یا کارمند و یا ارباب رجوع یک شرکت خاص بودن ما پوشیده بمانـد و ممکـن است دوباره در فعالیت‌های دیگر، ملزم به دادن مدارک یـا هویـت خـود باشیم. پالاینـده‌هـای نرم‌افزاری هم بیش از پیش دقیق شده و این توانایی را به ما می‌دهند که از خود و افـراد تحـت مراقبتمان در برابر اطلاعات ناخواسته از قبیل، مطالب نامطلوب نامه‌های مزاحم[1]، نـرم‌افزارهـای مغرض و دیگر اشکال خصومت مراقبت کنیم. به‌کارگیری و مدیریت این الزامـات مراقبتـی در درون شبکه‌های جدید اینترنت، هزینه‌های بسیاری برای بخش صـنعت و کـاربران در بـردارد. بنابراین، لازم است نوآوری و استفادهٔ تجاری از فناوری امنیتی و خدمات را ترغیب نمائیم.

طبیعتاً، رابط‌های زیرساخت ارتباطی مشترک و سـرورهای اسـامی نیـز دارای ابعـاد امنیتـی مختص به خود هستند. انتقال داده‌ها متکی به (رابط‌های) فیزیکی به‌گونه‌ای است که داده‌هـا از یک رایانه به رایانهٔ دیگر در طی مسیر هدایت می‌شوند. این رابطهـا بایـد در مکـانی مـستقر و

1. Spams

امنیت زیرساخت‌های اطلاعاتی

در جامعهٔ اطلاعاتی، شبکه‌هایی که توسط کاربران کنترل می‌شوند به‌تدریج جایگزین نسل قدیمی‌تر شبکه‌های ارتباطی ملی می‌گردند. یکی از دلایل موفقیت اینترنت، ایجاد امکان دسترسی کاربران به جدیدترین فناوری‌ها است. قانون مور[1] پیش‌بینی می‌کند که قدرت محاسبات رایانه‌ای هر ۱۸ ماه دو برابر شود.

با این وجود، فناوری ارتباطات با سرعتی حتی بیش از این در حال گسترش است. یکی از نتایج این توسعه دو برابر شدن حجم اطلاعات جابجا شده از طریق اینترنت در دوره‌هایی کمتر از یک‌سال است.

شبکه‌های تلفن کلاسیک از سوی سازمان‌های ملی راه‌اندازی و اداره می‌شدند. کاربران این شبکه‌ها، قدرت انتخاب اندکی نسبت به خدمات داشته و هیچ‌گونه کنترلی بر محیط ارتباطی نداشتند. به این ترتیب، اولین شبکه‌های داده‌ای بر مبنای همین فلسفهٔ محیط کنترل شده از مرکز بنا شدند که امنیت درون این شبکه‌ها مبین همین امر بود.

اما اینترنت و دیگر شبکه‌های ارتباطی جدید کاملاً متفاوت بوده و نگهداری از آنها باید برطبق این ماهیت متفاوت صورت بگیرد. کنترل و نظارت در این شبکه‌ها اغلب در حاشیه قرار می‌گیرد؛ یعنی جایی‌که کاربران و سرویس‌دهندگان حضور دارند. هستهٔ شبکه ساده و در عین حال کارآمد بوده و اساساً به کار انتقال داده‌ها مشغول است، کنترل و ارزیابی مختصری از محتوای مطالب موجود در شبکه صورت می‌گیرد. تنها در مقصد نهایی است که تکه‌های اطلاعاتی به آوای یک صدا، تصویر یک اشعهٔ x یا تأییدیهٔ یک مبادلهٔ بانکی تبدیل می‌شوند. بنابراین، نگهداری تا میزان قابل توجهی بر عهدهٔ کاربران است، زیرا تنها آنان می‌توانند ارزش و محتوای تکه‌هایی را که در حال دریافت یا فرستادن هستند، درک کرده و میزان مراقبت لازم را تعیین نمایند.

به این ترتیب کاربران بخشی مهمی از زیرساخت اطلاعاتی هستند، بنابراین تکنیک‌های

---

1. Moore

تحقیق و توسعه را که به‌منظور بالا بردن ضریب امنیت و اعتماد در زیرساخت‌های اطلاعاتی و مبادلات الکترونیکی به اجرا درآمده‌اند، حمایت می‌کرد.

همچنین این اتحادیه اخیراً بودجه مخصوص برنامهٔ مشابهی چون IST را افزایش داده است. پروژه‌های پژوهشی و اجرایی ویژه‌ای به‌منظور ارتقای مهارت‌های تخصصی پرسنل انتظامی و همچنین همکاری بین نیروی انتظامی و بخش صنعت انجام یافته که در چارچوب برنامه‌های ستون سوم از قبیل ایست[1] شاهین[2]، اویزین[3] و گروتیوس[4] مورد حمایت قرار گرفته‌اند.

طرح اجرایی مبارزه با جرائم سازمان‌یافته که توسط مجمع JHA در ماه می ۱۹۹۷ مورد پذیرش قرار گرفت و به تصویب شورای اروپا در آمستردام نیز رسید، شامل درخواستی برای مطالعه درخصوص جرائم مرتبط با رایانه توسط کمیسیون بود که باید تا پایان سال ۱۹۹۸ صورت می‌گرفت. این مطالعه (که اصطلاحاً مطالعه Comcrime نامیده می‌شود) از سوی کمیسیون در آوریل ۱۹۹۸ به گروه کاری چند ـ رشته‌ای که علیه جرائم سازمان‌یافته کار می‌کنند، پیشنهاد شد.

قبل از طرح این گفتار، کمیسیون مناسب دید که مشاوره‌ای غیررسمی با نمایندگانی از مراکز انتظامی و مراجع ناظر بر حفاظت اطلاعات کشورهای عضو و بخش صنعت اروپایی (به‌خصوص ISPها و عوامل ارتباط راه دور) به‌عمل آورد.

این گفتار بر مبنای تجزیه و تحلیل‌ها و پیشنهادات حاصل از مطالعه و نتایج به‌دست آمده از فرآیند مشاوره، امکاناتی که به‌دنبال معاهدهٔ آمستردام فراهم آمده‌اند و کارهایی که از قبل در اتحادیهٔ اروپایی، گروه ۸ و شورای اروپا، انجام شده‌اند، به بررسی گزینه‌هایی در زمینهٔ اقدامات آتی اتحادیه علیه جرائم رایانه‌ای می‌پردازد. در سطح اتحادیهٔ اروپا، راهکارهای منتخب نباید به ایجاد اخلال و از هم گسیختگی در بازار داخلی و یا به ایجاد ابزارهایی که به حقوق مسلم افراد لطمه وارد می‌کنند، منجر شوند.

---

1. Stop
2. Falcon
3. Oisin
4. Grotius

رایانه‌ای در سطوح ملی و فراملی به خوبی محرز گشته و سازمان‌های گوناگونی در حال هماهنگی یا تلاش برای هم‌سو نمودن این قبیل فعالیت‌ها بوده‌اند. وزرای دادگستری و کشورهای گروه ۸ (G8) در دسامبر ۱۹۹۷ مجموعه‌ای از اصول و یک طرح اجرایی ۱۰ مرحله‌ای را پذیرفتند که در نشست این گروه در ماه می ۱۹۹۸ در بیرمنگام انگلیس به تصویب رسیده و در حال حاضر نیز اجرا می‌شود. شورای اروپا در فوریهٔ ۱۹۹۷ تهیه و تدوین یک کنوانسیون در مورد جرائم سایبر را آغاز کرده و انتظار می‌رود که تا سال ۲۰۰۱ آنرا به اتمام رساند. همچنین مقابله با این جرائم، موضوع گفت‌وگوهای دوجانبه‌ای که کمیسیون اروپایی با برخی از دولت‌ها (غیر از کشورهای عضو اتحادیه) داشته، می‌باشد. یک طرح ضربتی مشترک هم بین ایالات‌متحده و کمیسیون اروپایی در زمینهٔ حفاظت از زیرساخت‌های حیاتی شکل گرفته است.

سازمان ملل متحد و سازمان همکاری و توسعهٔ اقتصادی (OECD) هم در این زمینه فعال بوده‌اند و این موضوع اخیراً در همایش‌های بین‌المللی از قبیل مذاکرات تجارت جهانی و تجارت فراآتلانتیکی نیز به بحث گذاشته می‌شود.

در سطح اتحادیهٔ اروپا، تا چندی پیش عملکرد قانونگذاری به‌طور عمده به شکل اقداماتی در زمینهٔ حمایت از حقوق ادبی، حفاظت از حقوق اساسی حریم خصوصی افراد، حمایت از داده خدمات دسترسی مشروط، تجارت الکترونیکی، امضاهای الکترونیکی و به‌ویژه برداشتن موانع و محدودیت‌ها در راه تجارت محصولات رمزنگاری، محدود می‌شد که همگی به‌طور غیرمستقیم با جرائم رایانه‌ای مرتبط هستند.

طی ۳ تا ۴ سال گذشته چند مورد معیار مهم غیر تقنینی نیز به‌کار گرفته شده که طرح اجرایی علیه نشر مطالب غیرمجاز و زیان‌آور بر روی اینترنت، شامل اقداماتی چون آگاه‌سازی، درجه‌بندی و کنترل یا فیلتر کردن محتوا، تلفن‌های قرمز و اقدامات اولیه‌ای در جهت حمایت از اقلیت‌ها و شرافت انسانی در جامعهٔ اطلاعاتی، جلوگیری از هرزه‌نگاری کودکان و شنود ارتباطات در راستای اجرای قانون، از آن جمله هستند. اتحادیهٔ اروپا از مدت‌ها پیش پروژه‌های

از این فناوری‌ها را نیز می‌طلبد. برخی از این فناوری‌ها از قبل موجود بوده‌اند، اما کاربران از وجود آنها یا روش استفاده از آنها ناآگاه بوده و یا حتی دلیل و توجیه لزوم به‌کارگیری آنها را هم نمی‌دانند.

واکنش‌های ملی و بین‌المللی

جرائم مرتبط با رایانه در پهنهٔ فضای سایبر رخ می‌دهند و در برخورد با مرزهای قراردادی ملل متوقف نمی‌شوند.

به‌طور کلی، این جرائم ممکن است در هر کجا و علیه هر کاربر رایانه‌ای در دنیا مورد ارتکاب واقع شوند، عموماً لزوم توجه به اقدامات مؤثر در مبارزه با جرائم رایانه‌ای در سطح ملی و بین‌المللی مشخص شده است. در سطح ملی، اقدامات فراگیر با گرایش بین‌المللی، نسبت به چالش‌های جدید ناشی از موضوع امنیت شبکه و جرائم رایانه‌ای اغلب وجود ندارد. در بیشتر کشورها، اقداماتی که علیه جرائم رایانه‌ای صورت می‌گیرد بر قوانین ملی آنها (به‌ویژه قوانین جزایی) متمرکز بوده و از توسل به جایگزین‌ها و عوامل بازدارنده غفلت شده است.

به‌رغم تلاش‌های سازمان‌های بین‌المللی و فراملی، قوانین ملی ابزارهای مختلف در سطح جهانی تفاوت‌های عمده‌ای به‌ویژه در مورد اصول قوانین کیفری مربوط به نفوذ به سیستم (Hacking)، حمایت از اسرار تجاری و نشر مطالب غیرمجاز وجود دارد. تفاوت‌های چشمگیری نیز در مورد اختیارات مراجع تحقیق (به‌ویژه در مورد اطلاعات رمزنگاری شده و پی‌جویی در شبکه‌های بین‌المللی)، محدودهٔ صلاحیت در مسائل جنایی و در مورد مسئولیت ارائه‌کنندگان خدمات واسطه از یک‌سو و تأمین‌کنندگان مطالب و محتوای شبکه از سوی دیگر وجود دارد. دستورالعمل ۳۱، سال ۲۰۰۰ کمیسیون اروپا در مورد تجارت الکترونیکی، این امر را در خصوص برخی از تأمین‌کنندگان خدمات واسطه و بعضی از فعالیت‌های آنها اصلاح کرده است. این توصیه‌نامه همچنین دولت‌های عضو اتحادیهٔ اروپا را از تحمیل مسئولیت کنترل و بررسی اطلاعاتی که از طریق آنها مبادله می‌شود، برحذر می‌دارد. لزوم مبارزه مؤثر با جرائم

زیرساخت اطلاعاتی[1] به بخش حساسی از شالوده اقتصاد ما تبدیل شده است. کاربران باید بتوانند به آسانی به در دسترس بودن خدمات اطلاعاتی اتکا کرده و این اطمینان را داشته باشند که ارتباطات و اطلاعات آنها از دسترسی و تحریف غیرمجاز در امان است. بهره‌برداری از تجارت الکترونیکی و توفیق کامل جامعه اطلاعاتی هم به این امر بستگی دارد.

فناوری‌های جدید دیجیتال و بی‌سیم[2] که اخیراً فراگیر شده‌اند، به ما آزادی تحرک و در عین حال همواره متصل بودن به منشوری از خدمات که در شبکه‌هایی از شبکه‌ها به‌وجود آمده‌اند را می‌دهند. آنها به ما امکان مشارکت، آموختن و فراگرفتن، کار و بازی کردن با هم و شرکت در جریان‌های سیاسی را می‌دهند. با اتکای روزافزون جوامع، ابزارهای عملی و حقوقی کارآمدی را برای کنترل عواقب آنها باید به‌کار گرفت.

فناوری‌های جامعهٔ اطلاعاتی می‌توانند برای انجام و یا تسهیل انواع فعالیت‌های جنایی به‌کار گرفته شده یا می‌شوند. این فناوری‌ها، در دست افرادی که با سوءنیت، غرض‌ورزی و اهمال‌کاری‌های بزرگی می‌کنند، به ابزاری تبدیل می‌شوند که زندگی، دارایی یا شأن و منزلت اشخاص را به خطر انداخته یا به منافع عمومی آسیب وارد می‌سازند. رهیافت سنتی امنیتی بر تفکیک دقیق سازمانی، جغرافیایی و ساختاری اطلاعات متکی بود، اما در دنیای دیجیتال این کار دیگر چندان میسر نیست، زیرا پردازش اطلاعات غیرمتمرکز[3] است، ارائه خدمات در دست کاربران متحرک بوده و قابلیت کنترل متقابل سیستم‌ها از الزامات شبکه می‌باشد. امروزه راه‌حل‌های نوظهور و هم‌سو با فناوری‌های رو به گسترش جایگزین روش‌های امنیتی سنتی می‌شوند.

این راه‌حل‌ها شامل؛ استفاده از رمزنگاری[4] و امضاهای دیجیتال، کنترل‌های دسترسی جدید، ابزارهای تصدیق هویت و فیلترهای نرم‌افزاری هستند. تضمین امنیت زیرساخت‌های اطلاعاتی مطمئن نه تنها مستلزم به‌کارگیری انواع فناوری‌هاست، بلکه به‌کارگیری درست و استفادهٔ مؤثر

---

1. Information Infrastructure
2. Wireless
3. Decentralization
4. Encoding

خواهد بخشید تا به فهم و کاهش آسیب‌پذیری‌ها منجر شده و به ترویج کاردانی و مهارت کمک کند.

این کمیسیون همچنین قصد دارد تا با ایجاد یک گردهمایی در اتحادیهٔ اروپا زمینه‌ای را به‌وجود آورد تا مراکز انتظامی، تأمین‌کنندگان خدمات اینترنتی، عوامل ارتباطات راه دور، سازمان‌های آزادی‌های فردی، نمایندگان مصرف‌کنندگان، مراجع حفاظت از اطلاعات و دیگر گروه‌های ذی‌نفع به‌منظور ارتقای درک مشترک و همکاری در سطح اروپا، گردهم آیند. این گردهمایی به‌دنبال افزایش سطح آگاهی مردم از خطراتی که مجرمان می‌توانند در اینترنت به‌وجود آورند، اتخاذ بهترین رویکرد در قبال امنیت، تشخیص بهترین ابزارهای مقابله با جرائم، روش‌هایی برای مقابله با جرائم رایانه‌ای، تقویت و گسترش بیشتر سازوکارهای مدیریت بحران و هشدار پیش از وقوع جرم، خواهد بود.

فرصت‌ها و تهدیدات در جامعه اطلاعاتی

ویژگی‌های عصر حاضر شامل روند رو به رشد توانایی و استفاده از فناوری‌های جامعهٔ اطلاعاتی (ISTS) و جهانی شدن اقتصاد است. توسعهٔ تکنولوژیکی و رشد به‌کارگیری شبکه‌های باز، مانند اینترنت، طی سال‌های آتی قابلیت‌های بیشتری را فراهم آورده و در عین حال چالش‌های تازه‌ای را نیز به‌دنبال خواهد داشت.

کمیسیون اروپایی در نشست مارس سال ۲۰۰۰ خود در لیسبون، بر اهمیت تبدیل شدن به یک اقتصاد پویا، رقابت‌زا و بر مبنای دانش روز تأکید داشته و از کمیسیون و شورا تدوین یک طرح اجرایی اروپای الکترونیکی برای برداشت حداکثر بهره‌برداری از این اقتصاد را خواستار شده است. این اقدام که توسط کمیسیون شورای اروپایی تدوین شده و در نشست شورا در ژوئن ۲۰۰۰ در فیرا مورد پذیرش قرار گرفت، شامل عملکردهایی در جهت افزایش امنیت شبکه و اتخاذ یک رویکرد یکسان و هماهنگ در خصوص جرائم رایانه‌ای تا پایان سال ۲۰۰۲ می‌شود.

همچنین خواستار ارائه تعاریف قابل پذیرشی از جرائم مرتبط با رایانه و وضع قوانین مؤثر مشابه، به‌ویژه در بخش حقوق جزای ماهوی شد. شورای اروپا در خصوص مذاکرات مقدماتی کنوانسیون جرائم رایانه‌ای موضع مشترکی را اتخاذ کرد و با تنی چند از اعضای خود به‌عنوان بخشی از استراتژی کلی اتحادیهٔ علیه جرائم مربوط به فناوری‌های پیشرفته را قبول کرد. برخی از کشورهای عضو اتحادیهٔ اروپا هم در انجام فعالیت‌های مربوط به گروه ۸، پیشتاز بودند.

در این گفتار، لزوم اتخاذ و اشکال ممکن یک سیاست جامع مبتکرانه برای دستیابی به جامعه اطلاعاتی گسترده‌تر و آزادی، امنیت و عدالت، به‌منظور بهبود امنیت زیرساخت‌های اطلاعاتی و مبارزه با جرائم رایانه‌ای اروپایی برای رعایت حقوق‌بشر، مورد توجه قرار گرفته است.

کمیسیون اروپا بر این باور است که در کوتاه‌مدت، اتحادیه اروپا نیازمند ابزاری برای تضمین کارآمدی ضمانت اجراهای کشورهای عضو علیه هرزه‌نگاری کودکان در اینترنت است. همچنین کمیسیون به‌زودی در سال‌جاری طراحی اتخاذ یک تصمیم چارچوبی را انجام خواهد داد که علاوه بر لحاظ کردن بستر گسترده‌تری در مباحث مربوط به سوءاستفاده جنسی از کودکان و قاچاق انسان، شامل دستورالعمل‌هایی برای همسان‌سازی قوانین و کیفرها نیز باشد.

در بلندمدت نیز این کمیسیون طرح‌های پیشنهادی قانونگذاری برای تصویب قوانین ماهوی کیفری همسان در مورد جرائم مربوط به فناوری پیشرفته را مطرح خواهد کرد. طبق نتایج نشست شورای اروپایی در تامپر در اکتبر سال ۱۹۹۹، کمیسیون همچنین گزینه‌هایی را برای به رسمیت شناختن متقابل اقدامات پیش‌گیرنده همسو با قانونگذاری‌ها در جرائم اینترنتی در نظر خواهد گرفت.

هم‌سو با این اقدامات، کمیسیون همچنین قصد تقویت و ایجاد واحدهای پلیس مخصوص جرائم رایانه‌ای در سطح ملی و در هر مکانی‌که چنین واحدهایی وجود نداشته باشند و حمایت از آموزش‌های فنی مناسب برای نیروهای انتظامی و تقویت اقدامات امنیتی ـ اطلاعاتی اروپایی را دارد. در سطح فنی و در راستای چارچوب قانونی هم، کمیسیون تحقیق و توسعه را ارتقا

کرده و جامعهٔ اطلاعاتی در تمامی ابعاد جامعه شیوع یافته است. در ژوئن سال ۲۰۰۰ شورای اروپایی (فیرا) طرح اقدام جامع اروپای الکترونیکی را پذیرفت و خواستار اجرای آن تا قبل از پایان سال ۲۰۰۲ شد. در این طرح، تأکید بسیاری بر اهمیت امنیت شبکه و لزوم مقابله با جرائم اینترنتی شده است.

زیرساخت‌های اطلاعاتی و ارتباطاتی به بخش عمده و حساسی از اقتصاد ما تبدیل شده‌اند. متأسفانه این زیرساخت‌ها هم آسیب‌پذیری‌های خاص خود را داشته و هم فرصت‌های تازه‌ای برای ارتکاب اعمال مجرمانه به‌وجود آورده‌اند. این فعالیت‌های مجرمانه ممکن است دارای اشکال گوناگونی بوده و جنبه فرامرزی داشته باشند. اگرچه، بنا بر دلایلی چند، آمار و ارقام موثقی در این خصوص وجود ندارد، اما شکی نیست که این جرائم تهدیدی علیه سرمایه‌گذاری‌های صنعتی، همچنین اعتماد و امنیت در جامعهٔ اطلاعاتی به‌شمار می‌روند. اخیراً وقوع چند مورد حملهٔ ویروسی و قطع خدمات Denial of Service منجر به وارد آمدن خسارات مالی گسترده‌ای شده، اما میدان عمل باز است، هم با بالا بردن سطح امنیت زیرساخت‌های اطلاعاتی می‌توان از فعالیت‌های مجرمانه جلوگیری کرد و هم می‌توان در عین حالیکه حقوق مسلم افراد کاملاً رعایت می‌شود، ترتیبی داد تا مراجع انتظامی و قضایی ابزار مناسب برای اقدام را داشته باشند.

اتحادیهٔ اروپایی اخیراً اقداماتی علیه نشر مطالب غیرقانونی و زیان‌آور، حفظ حقوق مالکیت معنوی و اطلاعات شخصی، ترویج تجارت الکترونیکی، استفاده از امضاهای الکترونیکی[1] و ارتقای امنیت معاملات انجام داده است. در آوریل ۱۹۹۸، کمیسیون نتایج مطالعه‌ای را که در مورد جرائم مربوط به رایانه صورت گرفته بود به شورای اروپا ارائه داد. (این مطالعه به اصطلاح COMCRIME نامیده می‌شود). در اکتبر ۱۹۹۹ شورای اروپایی در نشست خود در تامپر اعلام نمود که موضوع جرائم مربوط به فناوری‌های پیشرفته را باید در زمره اقداماتی که حصول توافق پیرامون تعاریف و مجازات‌های مشترک لازم است، قرار داد. پارلمان اروپایی،

---

1. Electronic Signatures

این همان رویکردی می‌باشد که از جانب توصیه شماره ۹(۸۹) و طرح گروه کاری OECD در سال ۱۹۸۵ اتخاذ شده است.

۵۰. کشورهای عضو می‌توانند رویکردی وسیع را اتخاذ کرده و فقط هک کردن را در انطباق با اولین جمله ماده ۲ جرم‌انگاری نمایند. از این‌رو اعضا می‌توانند هر یک یا تمامی عوامل تصدیق‌کننده که در دومین جمله ماده ۲ آمده است را به‌کار گیرند؛ نقض اقدامات امنیتی، سوءنیت خاص در کسب داده‌های کامپیوتری، سایر مقاصد سوء که قابلیت ارتکاب اعمال مجرمانه را محقق می‌سازد یا شرایطی که این جرم در ارتباط با سیستم که از راه دور به سیستم کامپیوتری دیگری متصل است، ارتکاب می‌یابد. آخرین راه چاره به اعضا اجازه داده تا وضعیتی را که در آن شخصی به‌صورت فیزیکی و بدون هیچ‌گونه استفاده‌ای از سیستم کامپیوتری دیگر به یک کامپیوتر مستقل دست پیدا کند را از شمول ماده ۲ مستثنی نمایند. آنها ممکن است جرم را محدود به دستیابی غیرقانونی به سیستم کامپیوتری متصل به شبکه کنند. (شامل شبکه‌های عمومی فراهم‌شده توسط خدمات مخابراتی و شبکه‌های خصوصی، نظیر اینترنت‌ها و اکسترانت‌ها).

ـ اروپا و جرائم رایانه‌ای

اروپا در گذر از ساختار سنتی به یک جامعه اطلاعاتی تحولات عظیمی را در تمامی ابعاد زندگی انسانی، پشت‌سر گذاشته است. تحول در بخش کار، آموزش و پرورش و تفریحات، ساختارهای دولتی، صنعت و تجارت از آن جمله‌اند. فناوری‌های نوظهور اطلاعاتی و ارتباطاتی تأثیری بنیادین و تحول‌زا بر اقتصاد جوامع ما داشته است. توفیق این جامعهٔ اطلاعاتی در رشد و توسعه جامعه اروپایی، ایجاد رقابت و فرصت‌های شغلی بسیار حائز اهمیت بوده و دارای آثار حقوقی، اجتماعی و اقتصادی گسترده‌ای می‌باشد.

کمیسیون اروپایی در دسامبر ۱۹۹۹ برای اولین بار طرح اروپای الکترونیکی (eEeurope) را به اجرا درآورد تا اطمینان یابد که اروپا می‌تواند از منافع فناوری‌های دیجیتال بهره‌برداری

۴۷. دستیابی، همچنین باید «به ناحق» انجام گیرد. علاوه بر توجیه ارائه شده در فوق، معنای این عبارت، آن است که دستیابی مجاز توسط مالک یا فرد دیگری که حق مالکیت آن سیستم یا بخشی از آنرا داراست، جرم محسوب نمی‌شود (برای مثال، دستیابی با هدف تست مجاز یا حفاظت از سیستم کامپیوتری مربوطه) به علاوه دستیابی به سیستم کامپیوتری که استفاده از آن به‌صورت رایگان برای عموم آزاد باشد، جرم محسوب نمی‌شود، بلکه چنین دستیابی «به حق» محسوب می‌شود.

۴۸. به‌کارگیری ابزارهای فنی خاص ممکن است منجر به دستیابی موردنظر ماده ۲ کنوانسیون و دستیابی به یک صفحه وب به‌صورت مستقیم یا از طریق ارتباطات فوق متن (Hyper Text Links) از جمله ارتباطات وسیع یا استفاده از کوکی‌ها (Cookies) یا بات‌ها (Bots) جهت یافتن محل اطلاعات مربوط به ارتباطات و دستیابی به آنها شود. استفاده از چنین ابزارهایی به خودی خود «ناحق» نیست. داشتن یک وب سایت عمومی حاکی از اجازه دارنده وب سایت برای دسترسی هر کاربر وب دیگر به آن است. استفاده از ابزارهای استاندارد فراهم شده از پروتکل‌های ارتباطات و برنامه‌های کاربردی معمول به خودی خود «ناحق» نیست، به‌ویژه در جایی‌که صاحب امتیاز و ذی‌حق سیستمی که دیگران به آن دست می‌یابند، می‌تواند درباره پذیرش برنامه‌های کاربردی‌اش تصمیم بگیرد، به‌عنوان مثال در مورد کوکی‌ها از طریق عدم پذیرش یا نصب اولیه یا پاک نکردن آنها تصمیم‌گیری می‌کنند.

۴۹. بسیاری از قانونگذاران ملی پیش از این نسبت به جرم Hacking دارای دیدگاه‌هایی بودند، اما چارچوب کلی و رویکرد آنها به شکل چشمگیری با یکدیگر متفاوت است. رویکرد وسیع جرم‌انگاری در اولین جمله ماده ۲ جای بحث دارد و مخالفت با آن ناشی از شرایطی است که خطراتی از جانب تجاوز صرف وجود نداشته یا حتی عمل هک منجر به شناسایی سوراخ‌های امنیتی[1] و ضعف‌های امنیتی سیستم‌ها می‌شود. در کشورهایی این موضوع به رویکردی ظریف‌تر منتهی شده که نیازمند شرایط تصدیق‌کننده و صلاحیت‌دار بیشتری است و

---

1. Security Holes

محرمانگی، صحت و موجودیت) سیستم‌ها و داده‌های کامپیوتری جزو آن به‌شمار می‌روند را شامل می‌شود. نیاز به حفاظت بیان کننده منافع سازمان‌ها و افراد در اداره، اجرا و کنترل سیستم‌های خود به شکل آزاد و منظم است.

صرف تجاوز غیرقانونی یک عمل هک (Hacking)، عمل کراک (Cracking) یا «تجاوز به حریم کامپیوتر» باید اصولاً و فی‌نفسه غیرقانونی تلقی شود. این جرائم ممکن است باعث ایجاد موانعی بر سر راه کاربران قانونی سیستم‌ها و داده‌ها شود و یا ممکن است تغییرات یا تخریباتی را که با هزینه‌های زیاد قابل بازسازی هستند، به‌وجود آورد. چنین تجاوزاتی ممکن است باعث دستیابی به اطلاعات محرمانه (شامل؛ گذر واژه‌ها و اطلاعات مربوط به سیستم‌های هدف) رمزهای سری، استفاده از سیستم بدون پرداخت پول یا حتی تشویق هکرها (Hackers) به انجام اشکال خطرناک‌تری از جرائم مربوط به کامپیوتر مانند کلاهبرداری کامپیوتری یا جعل کامپیوتری شود.

۴۵. مؤثرترین وسیله پیشگیری از دستیابی غیرمجاز، به‌کارگیری و توسعه اقدامات امنیتی مؤثر است. با این حال، وجود یک واکنش جامع و کامل برای تهدید بزهکاران بالقوه و استفاده از اقدامات حقوق جزا برای پیشگیری از دستیابی غیرمجاز را باید مدنظر داشت. منع کیفری دستیابی غیرمجاز قادر است از سیستم‌ها و داده‌ها حفاظت بیشتری کرده و در مراحل اولیه از آنها در برابر خطرات اشاره شده در بالا حفاظت کند.

۴۶. دستیابی، مشتمل بر ورود به کل یا جزئی از سیستم کامپیوتری است. (سخت‌افزار، تجهیزات جانبی، داده‌های ذخیره شده در سیستم نصب شده، فهرست‌های راهنما، داده‌های ترافیک و مربوط به محتوا). با این وجود، صرف ارسال یک پیام E-mail یا فایل به آن سیستم را دربر نمی‌گیرد. «دستیابی» شامل ورود به سیستم کامپیوتری دیگری که از طریق شبکه‌های ارتباطات عمومی به یک سیستم کامپیوتری و بر روی همان شبکه (مانند LAN شبکه محلی) یا اینترنت داخلی یک سازمان، می‌باشد که در این میان شیوه ارتباط (به‌عنوان مثال از فاصله دور از طریق ارتباطات بی‌سیم یا در یک دامنه بسته و نزدیک)، حائز اهمیت نیست.

را برای دولت‌ها و پارلمان‌ها در تعیین سیاست جزایی در این زمینه فراهم می‌آورد.

۴۱. قوانینی که این جرم‌انگاری‌ها براساس آنها است، باید تا حد امکان با دقت و ظرافت خاصی نوشته شوند تا قابلیت پیش‌بینی مناسب نوع رفتاری که منجر به محکومیت کیفری خواهد شد را فراهم سازند.

۴۲. طی فرآیند تهیه پیش‌نویس، پیش‌نویسان امکان شور در خصوص جرم‌انگاری رفتارهای دیگر، جدای از مواردی که در مورد ۲ تا ۱۱ تعریف شده را در نظر گرفتند، از جمله تملک غیرقانونی در فضای مجازی است. یعنی عمل ثبت نام یک حوزه (DOMAIN NAMES) یکسان با نام واحدی که قبلاً وجود داشته و معمولاً دارای شهرت بسیاری بوده و یا عیناً با یک نام تجاری یا علامت تجاری یک محصول یا شرکت تشابه دارد. عاملان تصرف غیرقانونی در محیط مجازی، قصد استفاده فعال از نام حوزه را نداشته و به‌دنبال کسب سود مالی، هرچند به‌طور غیرمستقیم و دریافت مبلغی جهت انتقال مالکیت نام حوزه هستند. این عمل در حال حاضر به‌عنوان یک مشکل مرتبط با علائم تجاری محسوب می‌شود. چون پرداختن به نقض علائم تجاری در حیطه این کنوانسیون نیست، پیش‌نویسان هم پرداختن به جرم‌انگاری این عمل را مناسب تشخیص نداده‌اند.

عنوان اول ـ جرائم علیه امنیت، صحت و موجودیت داده‌ها و سیستم‌های کامپیوتری

۴۳. جرائم کیفری احصا شده در مواد ۲ تا ۶ جهت حفاظت از محرمانگی، صحت و موجودیت سیستم‌ها یا داده‌های کامپیوتری و نه برای جرم‌انگاری فعالیت‌های قانونی و معمول در طراحی شبکه‌ها یا اقدامات تجاری یا عملیات قانونی و معمول در کنوانسیون جای داده شده‌اند.

ماده ۲ ـ دستیابی غیرمجاز

۴۴. دستیابی غیرقانونی، یک جرم اصلی است که تهدیدات خطرناک علیه امنیت (یعنی

می‌شود، استنباط می‌گردد، بنابراین بدون اعمال محدودیتی بر چگونگی به‌کارگیری مفهوم یادشده توسط کشورهای عضو از این مفهوم در حقوق داخلی خود احتمال دارد که آن مفهوم به رفتاری بدون مجوز (خواه قانونی، اجرایی، قضایی، قراردادی یا رضایی) یا رفتاری که تحت پوشش دفاع قانونی، معاذیر قانونی یا علل موجه قانونی، یا اصول مربوطه‌ای که در حقوق داخلی قرار نمی‌گیرد، اطلاق شود. بنابراین کنوانسیون فوق، اقدامات انجام‌شده با مجوز قانونی دولت‌ها را شامل نمی‌شود، بلکه اقدام دولت عضو در جهت برقراری نظم عمومی یا حمایت و حفاظت از امنیت ملی یا انجام تحقیقات جنایی، از جمله این موارد است. به‌علاوه، فعالیت‌های قانونی و معمول در طراحی شبکه‌ها یا عملیات قانونی و معمول یا فعالیت‌های تجاری نباید جرم‌انگاری محسوب شوند. نمونه‌های خاصی از این استثنائات در رابطه با جرائم خاص در بخش مربوطه از یادداشت توجیهی ذیل بیان شده است. مشخص کردن چنین استثنائاتی براساس سیستم قانونی کشورهای عضو به خود آنان واگذار شده است. (در حقوق جزا یا موارد دیگر)

۳۹. تمامی جرائم گنجانده‌شده در کنوانسیون باید از روی عمد انجام شده باشند تا مسئولیت جزایی درباره مرتکب قابل اعمال باشد. در مواردی خاص، وجود یک عنصر عمد خاص مکمل برای تحقق جرم ضروری است.

مثلاً در ماده ۸ کلاهبرداری مرتبط با کامپیوتر، قصد کسب بهره اقتصادی عنصر سازنده این جرم است. پیش‌نویسان این کنوانسیون به این توافق رسیدند که تفسیر مفهوم دقیق «از روی عمد» بایستی بر عهده حقوق ملی گذاشته شود.

۴۰. برخی از موارد در این بخش به کشورهای عضو اجازه افزودن شرایطی را هنگام اجرای کنوانسیون در کشورشان براساس حقوق داخلی می‌دهد. در سایر موارد، حتی احتمال محفوظ نگه‌داشتن حق در نظر گرفته (مواد ۴۰ و ۴۲) شده است. روش‌های متفاوت در رویکرد محدودتر جرم‌انگاری، نشان‌دهنده ارزیابی‌های مختلفی از خطرناکی رفتار مربوطه یا نیاز به کاربرد حقوق جزایی به‌عنوان یک اقدام مقابله‌ای است. این رویکرد، انعطاف‌پذیری لازم

آزادی بیان را ابراز می‌داشتند. با توجه به پیچیدگی موضوع، تصمیم بر آن شد که کمیته مذکور به کمیته اروپایی، مشکلات جزایی (CDPC) موضوع را منعکس کند و تدوین پروتکل الحاقی در همین خصوص را خواستار شود.

۳۵. عنوان چهارم به جرائم نقض کپی رایت[1] و حقوق مربوط به آن اختصاص دارد. به همین دلیل در کنوانسیون عنوان شد که نقض کپی رایت یکی از گسترده‌ترین اشکال جرائم کامپیوتری مرتبط با کامپیوتر می‌باشد و افزایش آن، توجه بین‌المللی را به خود جلب کرده است.

در نهایت، عنوان پنجم شامل امکانات اضافی درباره شروع به جرم، مساعدت و معاونت در جرم، مجازات‌ها و معیارها بوده و استفاده از ابزارهای بین‌المللی جدید پیرامون مسئولیت شرکت‌ها را هم شامل می‌شود.

۳۶. اگرچه مواد حقوق جزای ماهوی با جرائمی که با استفاده از تکنولوژی اطلاعات واقع می‌شوند، مرتبط است، اما این کنوانسیون از ادبیات بی‌طرفانه تکنولوژی استفاده می‌کند، به طوری‌که جرائم حقوق جزای ماهوی بتوانند در باب تکنولوژی فعلی و آینده نیز کاربرد داشته باشند.

۳۷. پیش‌نویسان کنوانسیون بر این موضوع توجه داشته‌اند که اعضا ممکن است تخلفات جزئی یا قابل اغماض را از شمول جرائم تعریف‌شده در موارد ۲ الی ۱۰ مستثنی کنند.

۳۸. ویژگی جرائم گنجانده‌شده در کنوانسیون که به صراحت بیان شده نشانه آن است که رفتار مربوطه باید به ناحق صورت گرفته باشد. حالت یادشده بیانگر این بینش است که رفتار توصیف‌شده همیشه، فی‌نفسه قابل مجازات نیست و ممکن است نه تنها در مواردی، قانونی یا موجه بوده و اصول مرتبط با قوانین سنتی مانند توافق، دفاع مشروع یا ضرورت، درباره مرتکب قابل اعمال باشد بلکه در مواردی هم اصول یا انگیزه‌های دیگر می‌تواند منجر به زوال مسئولیت مجرمانه مرتکب شود. مفهوم اصطلاح «به ناحق» از شرایطی که در آن به‌کار گرفته

---

1. Copy Right

۳۲ـ جرائم مندرج در کنوانسیون مربوط، نشانگر یک توافق حداقل است که از بسط و توسعه آن در حقوق داخلی ممانعت نمی‌کند. این امر تا حد زیادی مبتنی بر راهبردهای توصیه شماره ۹ (R ۸۹) شورای اروپا پیرامون جرائم مربوط به کامپیوتر و عملکرد دیگر سازمان‌های بین‌المللی عمومی و خصوصی (OECD, UN, AIDP) است، اما تجارب پیشرفته‌تری که از برخورد با سوءاستفاده از توسعه شبکه‌های ارتباطات راه دور حاصل شده را نیز در نظر می‌گیرد.

۳۳ـ این بخش، تحت پنج عنوان مطرح می‌شود؛ عنوان اول، شامل قسمت عمده‌ای از جرائم مربوط به کامپیوتر می‌باشد که حاکی از تهدیدات جدی هستند که در مبحث کامپیوتر و امنیت داده‌ها بوده و پردازش داده‌های الکترونیک و سیستم‌های ارتباطی را شامل می‌شوند. این عنوان، جرائمی را تشریح می‌کند که شامل دستیابی غیرقانونی به سیستم‌ها، داده‌ها، برنامه‌ها و مختل کردن غیرقانونی آنها می‌شود.

عناوین دوم تا چهارم، شامل انواع دیگر جرائم مربوط به کامپیوتر است که عملاً نقش بیشتری ایفا می‌کنند و سیستم‌های ارتباطات راه دور و کامپیوتر به‌عنوان وسایلی جهت تعرض به منافع قانونی را دربرمی‌گیرد. جرائم عنوان دوم (کلاهبرداری و جعل مرتبط با کامپیوتر) براساس پیشنهادات مطرح‌شده در توصیه‌های راهبردی شماره ۹ (R ۸۹) شورای اروپا به کنوانسیون افزوده شده‌اند.

۳۴. عنوان سوم، شامل جرائم مرتبط با محتوا از قبیل تولید یا پخش غیرقانونی تصاویر مستهجن از کودکان با استفاده از سیستم‌های کامپیوتری به‌عنوان یکی از خطرناک‌ترین روش‌های ارتکاب جرم است. کمیته‌ای که تهیه پیش‌نویس این کنوانسیون را بر عهده داشت، در مورد شمول این موضوع بر سایر جرائم مرتبط با محتوا مانند توزیع تبلیغات نژادپرستانه با استفاده از سیستم‌های کامپیوتری نیز به مباحثه پرداخت. با این وجود، کمیته مذکور بر سر جرم‌انگاری چنین رفتارهایی به توافق نرسید، چراکه برخی از کشورها حمایت چشمگیری از جرم‌انگاری این رفتارها می‌کردند، اما نمایندگان برخی از کشورها، نگرانی جدی خود از تهدید

آنها خواهد بود. «اصل» به مبدأ شماره تلفن، آدرس پروتکل اینترنت (IP) یا هویت مشابه در وسیله ارتباطی که تأمین‌کننده خدمات به‌وسیله آنها خدمات ارائه می‌دهد، اطلاق می‌شود. مقصد به شاخص مشابه در وسیله ارتباطی اطلاق می‌گردد که ارتباط با آنجا برقرار می‌شود. اصطلاح «نوع سرویس زیربنایی» به‌نوع خدماتی که در شبکه مورد استفاده قرار می‌گیرد، مانند انتقال فایل، پست الکترونیکی یا ارسال پیام فوری[1] اطلاق می‌شود.

۳۱. این تعریف، قانونگذاران ملی را وادار کرده تا تفاوت‌های خاص در حمایت قانونی از داده‌های ترافیک را با توجه به حساسیت آنها قائل شوند. در این زمینه ماده ۱۵، کشورهای عضو را مجبور ساخته تا شرایط و زمینه‌های حمایت از حقوق‌بشر و آزادی را فراهم سازند.

ـ گزارش توجیهی کنوانسیون بوداپست

۳۰ـ فصل دوم (مواد ۲ تا ۲۲) شامل ۳ بخش است:

حقوق جزای ماهوی (ماده‌های ۲۲ تا ۱۳)، آیین دادرسی (۲۱ تا ۱۴) و صلاحیت (ماده ۲۲)

بخش ۱ـ حقوق جزای ماهوی

۳۱ـ هدف بخش اول این کنوانسیون (مواد ۲ـ۱۳) ارتقا و پیشرفت وسایل پیشگیری و متوقف ساختن جرائم کامپیوتری یا مرتبط با کامپیوتر از طریق ایجاد حداقل استانداردهای معمول جرائم مربوطه است. این نوع هماهنگی، باعث تسهیل مبارزه با چنین جرائمی در سطح بین‌المللی و ملی می‌شود. همگرایی در حقوق داخلی کشورها ممکن است از سوءاستفاده‌هایی که از تبدیل شدن یک کشور به یک عضو با استانداردهای پایین قبلی شود، پیشگیری کند. در نتیجه، مبادله تجارب مشترک و مفید حاصله از برخورد عملی با پرونده‌ها نیز ممکن است، افزایش یابد. همکاری بین‌المللی (مانند استرداد و همکاری متقابل قضایی) مثلاً در ارتباط با مقتضیات و مقررات مجرمیت مضاعف تسهیل می‌شود.

---

1. Immediate Message

با این وجود، یک تأمین‌کننده محتوای صرف (مانند شخصی که با یک شرکت میزبان وب جهت میزبانی سایت وب قرارداد می‌بندد) در صورتی‌که اقدام به ارائه خدمات ارتباطی یا پردازش داده‌های مربوطه نکند، مشمول این تعریف نخواهد شد.

ماده ۱ـ (D) داده‌های ترافیک[1]

۲۸. برای اهداف این کنوانسیون، داده‌های در حال جابجایی که در بند D از ماده ۱ تعریف شده‌اند، دسته‌ای از داده‌های کامپیوتری هستند که مشمول نظام حقوق خاصی می‌گردند. این داده‌ها توسط کامپیوترها در زنجیره ارتباطات تولید می‌شوند تا ارتباطی را از مبدأ تا مقصد، مسیریابی کنند. بنابراین داده‌های یادشده برای مساعدت در ایجاد ارتباطات پدید می‌آیند.

۲۹. موارد پی‌جویی جرائم ارتکاب یافته در ارتباط با سیستم کامپیوتری، سرنخی برای جمع‌آوری مدارک بیشتر و ردیابی مبدأ ارتباط به‌عنوان بخشی از مدارک جرم محسوب می‌شوند. دوام و پایداری داده‌های ترافیک ممکن است فقط به‌صورت موقتی باشد که اتخاذ تدابیر مناسب جهت حفظ و نگهداری فوری آن ضروری است، در نتیجه اظهار و افشای سریع آن برای تعیین مسیر ارتباط در جهت جمع‌آوری مدارک بیشتر قبل از اینکه حذف شوند یا از بین روند، برای شناسایی لازم است. بنابراین روش‌های مشمول جمع‌آوری و افشای ادله داده‌های کامپیوتری ممکن است، کافی نباشد. به‌علاوه نحوه جمع‌آوری این داده‌ها به‌گونه‌ای است که چندان حالت فضولی ندارد، زیرا محتوای ارتباط را که حساس‌تر و مهم‌تر هستند، فاش نمی‌کند.

۳۰. این تعریف به‌طور کامل فهرست انواع داده‌های ترافیک که در این کنوانسیون مشمول نظام حقوقی خاصی می‌شوند را مشخص می‌کند. مبدأ ارتباط، مقصد، مسیر، زمان، (GMT) تاریخ، اندازه، مدت زمان و نوع خدمات اصلی همیشه از لحاظ فنی در دسترس نخواهند بود، بلکه قابلیت تهیه آنها توسط تأمین‌کننده خدمات یا نیاز در تحقیقات جنایی خاص سبب تهیه

1. Traffic Datas

می‌شوند که بتوان آنها را از طریق سیستم کامپیوتری مستقیماً پردازش نمود. برای آنکه روشن شود داده‌های موردنظر این کنوانسیون بایستی به‌صورت الکترونیک یا اشکال دیگر قابل پردازش مستقیم باشند، از واژه داده‌های کامپیوتری استفاده شده است. داده‌های کامپیوتری که به‌صورت خودکار پردازش می‌شوند، ممکن است هدف یکی از جرائم تعریف‌شده در این کنوانسیون قرار گیرند، همان‌طور که می‌توانند موضوع اقدامات و معیارهای تحقیقی تعریف‌شده در این کنوانسیون واقع شوند.

ماده ۱ـ (C) تأمین‌کننده خدمات

۲۶. واژه (تأمین‌کننده خدمات) مشتمل بر گروه وسیعی از افراد می‌شود که نقش خاصی با توجه به ارتباط یا پردازش داده‌ها بر روی سیستم کامپیوتری ایفا می‌کنند (CF نیز بخش ۲ را تحلیل و تفسیر می‌کند.) براساس بخش (۱) تعریف، بدیهی است که هم سازمان‌های شخصی و هم عمومی که برای کاربران امکان برقراری ارتباط با یکدیگر را فراهم می‌آورند را نیز شامل می‌شود.

بنابراین خواه کاربران منحصر به گروهی خاص و محدود باشند یا اینکه تأمین‌کننده خدمات خود را به عموم ارائه دهند و خواه به‌صورت مجانی یا با دریافت هزینه، هیچ تفاوتی نمی‌کنند، این گروه خاص و محدود می‌توانند، مانند کارمندان یک بخش خصوصی باشند که خدمات از طریق شبکه کامپیوتری شرکت به آنها ارائه می‌شود.

۲۷. در بخش دوم تعریف یاد شده این موضوعات روشن می‌شود که واژه تأمین‌کننده خدمات، شامل افرادی که داده‌ها را برای افراد یاد شده در بخش اول ذخیره کرده یا پردازش می‌کند، هم می‌شود. به‌علاوه واژه فوق شامل آن دسته از افرادی هم می‌شود که داده‌ها را برای کاربران خدمات، آنهایی که در بخش ۱ به آنها اشاره شد، ذخیره یا پردازش می‌کنند. به‌عنوان مثال، براساس این تعریف، تأمین‌کننده خدمات، هم شامل خدمات میزبانی و ذخیره و هم شامل خدمات اتصال به شبکه می‌شود.

منظور از (اتوماتیک) این است که انسان دخالت مستقیمی در آن ندارد. (پردازش داده‌ها)[1] یعنی اینکه داده‌های داخل سیستم کامپیوتری از طریق اجرای یک برنامه کامپیوتری فعال می‌شوند. یک برنامه کامپیوتری؛ مجموعه‌ای از دستورات است که کامپیوتر می‌تواند آنها را در جهت دستیابی به نتیجه موردنظر اجرا نماید. یک کامپیوتر می‌تواند برنامه‌های مختلفی را انجام دهد. سیستم کامپیوتری معمولاً متشکل از وسایل متفاوتی بوده که به‌صورت پردازنده یا واحد پردازش مرکزی و وسایل جانبی هستند. یک (وسیله جانبی) دستگاهی است که وظایف خاصی را در تعامل با واحد پردازنده مانند پرینتر، صفحه مانیتور، خواننده (reader) یا سی‌دی خوان، رایتر سی دی یا دیگر وسایل ذخیره اطلاعات انجام می‌دهد.

۲۴. یک شبکه ارتباط و اتصال ما بین دو یا چند سیستم کامپیوتری است. ارتباطات ممکن است زمینی (مانند سیستم یا کابل)، بی‌سیم (رادیو، مادون‌قرمز یا ماهواره) یا مرکب از هر دو مورد باشد. شبکه ممکن است از لحاظ جغرافیایی منطقه کوچکی (شبکه‌های محلی) یا منطقه بزرگی (شبکه‌های وسیع) را احاطه کند و حتی ممکن است چنین شبکه‌هایی خودشان به یکدیگر متصل باشند. اینترنت، شبکه جهانی متشکل از شبکه‌های متصل بسیاری است که همگی از پروتکل‌های یکسانی استفاده می‌نمایند. انواع دیگری از شبکه‌ها نیز وجود دارند که خواه متصل به اینترنت باشند یا نباشند، قادرند تا داده‌های کامپیوتری در بین سیستم‌های کامپیوتری را راه انداخته و به‌یکدیگر ارتباط دهند. برخی سیستم‌های کامپیوتری ممکن است به‌عنوان نقاط پایانی یا به‌عنوان وسیله‌ای کمکی متصل یا به شبکه مرتبط باشند. آنچه حائز اهمیت می‌باشد، این است که داده‌ها بر روی شبکه با یکدیگر مبادله می‌شوند.

ماده ۱ـ (b) داده‌های کامپیوتری[2]

۲۵. تعریف داده‌های کامپیوتری براساس تعریف ISO از داده‌ها صورت گرفته است. این تعریف دربردارنده واژه مناسبی برای پردازش می‌باشد. یعنی اینکه داده‌ها به شکلی ارائه

---

1. Process of Datas 2. Database

اول: زمانی که پایه و اساسی قانونی (پیمان، قانون رفتار متقابل و غیره) برای همکاری ما بین دو طرف وجود ندارد و دوم: در صورتی است که چنین پایه و اساسی وجود دارد، ترتیبات موجود مطابق این کنوانسیون قابل اعمال می‌باشد.

همکاری خاص در زمینه مبارزه با جرائم کامپیوتری و جرائم مربوط به کامپیوتر در هر دو حالت قابل اعمال است و در سایر شرایط، اختیارات آئین دادرسی را همان‌طور که در فصل دوم بیان شده است، شامل می‌شود. به‌علاوه فصل سوم، حاوی مبحثی پیرامون نوع خاصی از دستیابی فرامرزی به داده‌های کامپیوتری ذخیره شده است که نیازی به همکاری متقابل ندارد.

۲۱. در نهایت فصل چهارم، مشتمل بر موضوعات پایانی است که با یک سری استثنائات خاص، موضوعات استاندارد در معاهدات شورای اروپا را تکرار می‌کند.

تفسیر مواد کنوانسیون

فصل ۱ـ کاربرد واژه‌ها

درآمدی بر تعاریف در ماده ۱

۲۲. تهیه‌کنندگان پیش‌نویس دریافتند که براساس این کنوانسیون، اعضا مجبور نیستند تا چهار مفهومی را که در ماده ۱ تعریف شده است کاملاً و عیناً به حقوق و قوانین خود اضافه کنند، به شرط اینکه قوانین داخلی آنها دارای مفاهیمی هماهنگ با اصول و مفاد این کنوانسیون باشد و چارچوبی معادل را برای اجرای آن ارائه دهند.

ماده ۱ـ (a) سیستم کامپیوتری

۲۳. سیستم کامپیوتری موردنظر این کنوانسیون، وسیله‌ای متشکل از نرم‌افزار و سخت‌افزار است که به‌منظور پردازش اتوماتیک داده‌های دیجیتالی تهیه شده و ممکن است شامل ورودی و خروجی و تسهیلات ذخیره اطلاعات باشد، سیستم کامپیوتری ممکن است تنها یا به شبکه‌ای از دیگر وسایل مشابه متصل باشد.

۱۷. از این رو کنوانسیون شامل ۴ فصل می‌شود؛

۱. استفاده از اصطلاحات

۲. اقدامات داخلی کشورهای عضو

۳. قوانین ماهوی و قانون آئین دادرسی

۴. فصل پایانی

۱۸. بخش اول از فصل دوم مسائل و موضوعات قانون ماهوی، جرم‌انگاری و همچنین سایر مسائل.مربوطه در حوزه جرائم کامپیوتری یا مربوط به کامپیوتر را شامل می‌شود، این بخش ابتدا ۹ جرم که در ۴ گروه مختلف قرار دارند را توضیح داده و سپس به مسئولیت کیفری می‌پردازد. جرائم زیر توسط کنوانسیون تعریف شده‌اند که عبارتند از:

دسترسی غیرقانونی، شنود غیرقانونی، اختلال در داده‌ها، اختلال در سیستم، سوءاستفاده از وسایل و تجهیزات، جعل مرتبط با کامپیوتر، کلاهبرداری مرتبط با کامپیوتر، جرائم مربوط به حقوق پدیدآورندگان و حقوق همجواری.

۱۹. بخش دوم از فصل دوم (مشکلات آئین دادرسی) حوزه و چارچوب این بخش فراتر از جرائم تشریح شده در بخش اول است، چراکه این بخش هر جرم ارتکاب یافته با سیستم کامپیوتری یا ادله کامپیوتری که به شکل الکترونیک باشد را شامل می‌شود. ابتدا، شرایط معمول و اقدامات امنیتی را که قابل اعمال در تمامی بخش‌های اختیارات دادرسی در این فصل هستند، تعیین شده است. سپس اختیارات شکلی که موجب حفاظت از داده‌های ذخیره شده به‌طور مؤثر می‌باشد، حفاظت مؤثر و شدید و افشای جزئی داده‌های حاصله از انتقال داده‌ها، سفارش تولید، تفتیش و توقیف داده‌های کامپیوتری، جمع‌آوری همزمان داده‌های در حال انتقال با شنود محتوای داده‌ها را مشخص می‌نماید و فصل دوم با بیان صلاحیت‌ها پایان می‌یابد.

۲۰. فصل سوم حاوی موضوعات مرتبط با همکاری متقابل بین‌المللی در خصوص جرائم سنتی و کامپیوتری علاوه بر مقررات مربوط به استرداد است. این فصل، همکاری متقابل سنتی را از دو لحاظ تحت پوشش خود قرار می‌دهد؛

حمایت خود را از فعالیت PC-CY از طریق اتخاذ یک موضع مشترک در ماه مه سال ۱۹۹۹ اعلام داشتند.

۱۳. کمیته PC-CY 10 جلسه را بین آوریل و دسامبر ۲۰۰۰ به‌طور کامل و ۱۵ پیش جلسه گروه پیش‌نویس را برگزار نمود. به‌دنبال خاتمه مدت مهلت اعطایی به کمیته، متخصصان و کارشناسان تحت حمایت کمیته CDPC سه جلسه بیشتر جهت تکمیل پیش‌نویس کنوانسیون و یادداشت توجیهی تشکیل دادند و پیش‌نویس کنوانسیون را با کمک و نظر انجمن پارلمانی مورد بررسی قرار دادند. کمیته آرا در اکتبر ۲۰۰۰ از انجمن یاد شده درخواست کرد تا نظراتش را پیرامون پیش‌نویس کنوانسیون ارائه دهد که انجمن هم در دومین بخش جلسه عمومی خود در آوریل ۲۰۰۱ آنرا تصویب کرد.

۱۴. به‌دنبال تصمیم اتخاذ شده از جانب کمیته PC-CY نسخه اولیه پیش‌نویس کنوانسیون از حالت محرمانه خارج شد و در آوریل ۲۰۰۰ منتشر گردید که به‌دنبال آن پیش‌نویس‌های پی‌درپی دیگری نیز پس از هر اجلاس عمومی منتشر شد تا کشورهای مذاکره‌کننده را قادر سازد با تمامی طرف‌های ذینفع مشورت نمایند. این فرآیند مشاوره مفید واقع شد.

۱۵. پیش‌نویس کنوانسیون تصحیح شد و اتمام یافت و یادداشت توجیهی آن جهت تأیید در پنجاهمین جلسه عمومی در ژوئن ۲۰۰۱ تسلیم کمیته CDPC شد که به‌دنبال آن متن پیش‌نویس کنوانسیون به کمیته وزرا جهت تصویب و امضا تسلیم گردید.

۱۶. اهداف کنوانسیون که به‌طور عمده شامل موارد ذیل می‌شود، عبارتند از:

الف) هماهنگ کردن ارکان تشکیل‌دهنده جرم در حقوق جزای ماهوی داخلی کشورها و مسائل مربوطه در بخش جرائم سایبراسپیس.

ب) فراهم‌آوردن اختیارات لازم آئین دادرسی کیفری داخلی برای پی‌جویی و تعقیب جرائمی که با استفاده از سیستم‌های کامپیوتری ارتکاب می‌یابند یا مدرک مرتبط با جرم به شکل الکترونیکی است.

ج) تدوین سیستم سریع و مؤثر همکاری بین‌المللی.

این کمیته بایستی تا حد امکان سند قانونی اتصال‌دهنده‌ای را برای موارد ۱ تا ۵ با تأکید ویژه بر مسائل بین‌المللی و در صورت مقتضی توصیه‌های جانبی در ارتباط با موضوعات خاص تهیه نماید، همچنین این کمیته ممکن است پیشنهاداتی در رابطه با سایر موضوعات مرتبط با پیشرفت‌های فناوری نیز ارائه دهد.

۱۲. علاوه بر تصمیم CDPC، کمیته وزرا کمیته جدیدی را به نام کمیته متخصصان جرائم سایبر اسپیس (PC-CY) براساس تصمیم شماره ۵۸۳ (Dec/Del/CM97) اتخاذ شده در پانصد و هشتاد و سومین نشست جانشینان وزرا (در ۴ فوریه ۱۹۹۷) تشکیل داد. کمیته PC-CY کار خود را در آوریل ۱۹۹۷ شروع کرد و مذاکراتی را پیرامون پیش‌نویس کنوانسیون جرائم سایبر اسپیس به عمل آورد. این کمیته در چارچوب حدود اختیارات خاص خود مصمم بود تا فعالیتش را تا ۳۱ دسامبر ۱۹۹۹ به اتمام رساند.

از آنجایی‌که کمیته تا آن زمان هنوز در شرایطی قرار نداشت تا به‌طور کامل از مذاکرات خود پیرامون مسائل خاصی که در پیش‌نویس کنوانسیون وجود داشته، نتیجه‌گیری کند، بنابراین ادامه کار آن توسط تصمیم شماره ۶۷۹ (Del/CM/Dec۹۹) جانشینان وزرا تا تاریخ ۳۱ دسامبر ۲۰۰۰ تمدید شد. وزرای دادگستری اروپایی دوباره حمایت خود را توسط قطعنامه شماره (۱) که در بیست‌ویکمین کنفرانس آنها به تصویب رسیده بود (پراگ ژوئن ۱۹۹۷) اعلام داشتند و به کمیته پیشنهاد کردند تا از کار انجام شده توسط CDPC پیرامون جرائم سایبر اسپیس در جهت تقریب و نزدیکی مقررات و شرایط حقوق جزا به یکدیگر و استفاده از وسایل مؤثر پی‌جویی چنین جرائمی پشتیبانی کنند.

علاوه بر این در قطعنامه شماره (۳)، بیست و سومین کنفرانس وزرای دادگستری اروپا، طرف‌های مذاکره کننده را تشویق می‌کرد، تا تلاش‌های خود را با دیدگاه یافتن راه‌حل‌های مناسب دنبال کنند تا در نتیجه تعداد زیادی از کشورها قادر باشند در این کنوانسیون شرکت نمایند و نیاز به وجود یک سیستم سریع و مؤثر همکاری بین‌المللی با تکیه بر نیازهای خاص مبارزه با جرائم سایبر اسپیس را مطابق با زمان درک کنند. کشورهای عضو اتحادیه اروپا،

۱۱. حدود اختیارات خاص کمیته جدید به‌صورت ذیل بود؛

با عنایت به توصیه شماره ۹ ((۸۹)R) پیرامون جرائم کامپیوتری و توصیه شماره ۱۳ ((۹۴) R) در رابطه با مشکلات آئین دادرسی کیفری مرتبط با فناوری اطلاعات، کمیته باید به‌صورت ویژه‌ای در زمینه موضوعات زیر بررسی نماید:

الف. جرائم رایانه‌ای به‌ویژه مواردی که با استفاده از شبکه‌های ارتباطات راه دور مانند اینترنت، ارتکاب می‌یابد، نظیر مبادلات مالی غیرقانونی، نقض حقوق پدیدآورندگان و همچنین اقداماتی که شأن و کرامت انسانی را مورد تهدید قرار می‌دهد و همچنین تخلف از قوانین حامی کودکان.

ب. سایر مسائل حقوق جزای ماهوی که در تعیین رویکردی عام در زمینه تعاریف، مجازات‌ها و مسئولیت عاملان در محیط مجازی از جمله مسئولیت تأمین‌کنندگان خدمات اینترنت که برای گسترش همکاری بین‌المللی لازم است.

ج. استفاده و همچنین امکان‌پذیر بودن استفاده فرامرزی و کاربرد عملی اختیارات اجباری در محیط تکنولوژیکی مانند؛ شنود ارتباطات، مراقبت الکترونیکی در شبکه‌های اطلاعات مثلاً از طریق اینترنت، تفتیش و توقیف در سیستم‌های پردازنده اطلاعات (از جمله سایت‌های اینترنتی) غیرقابل دسترس ساختن موارد غیرقانونی، لزوم تدوین تعهداتی خاص برای ارائه‌کنندگان خدمات و مدنظر قرار دادن مشکلات و مسائلی که به‌واسطه اقدامات ویژه مرتبط با امنیت اطلاعات مانند رمزنگاری پدید می‌آید.

د. مسئله صلاحیت در جرائم فناوری اطلاعات، به‌عنوان مثال تعیین مکانی که جرم ارتکاب یافته است، در تعیین اینکه کدام قانون باید اعمال شود و همچنین مشکل اعتبار امر مختوم در حالت وجود صلاحیت‌های متعدد و مسئله نحوه برطرف کردن تعارض‌های مثبت در صلاحیت‌ها و نحوه اجتناب از تعارض‌های منفی در صلاحیت‌ها.

ذ. مسائل مربوط به همکاری‌های بین‌المللی در پی‌جویی جرائم واقعه در محیط مجازی و ارتباط نزدیک با کمیته کارشناسان عملیاتی کنوانسیون‌های اروپایی در زمینه جزایی.(PC-OC)

سرویس‌های اطلاعات و ارتباطات نوعی فضای عام به نام «سایبر اسپیس»[1] را پدید می‌آورند که برای مقاصد قانونی به‌کار می‌رود، اما این فضا ممکن است مورد سوءاستفاده نیز واقع شود. جرائم در محیط رایانه‌ای ممکن است علیه ثبات، موجودیت و قابلیت اطمینان به سیستم‌های کامپیوتری در شبکه‌های ارتباط راه دور رخ دهند یا اینکه از خدمات ارائه شده در جهت ارتکاب جرائم سنتی استفاده شود. ماهیت فرامرزی چنین جرائمی مثلاً در صورتی‌که از طریق اینترنت ارتکاب یابند، در تضاد با صلاحیت سرزمینی نیروهای پلیس است.

۹. بنابر.این حقوق جزا باید این پیشرفت‌های تکنولوژیکی که فرصت‌های بسیار پیچیده‌ای جهت سوءاستفاده از تسهیلات سایبراسپیس و وارد آوردن آسیب به منافع قانونی را فراهم می‌آورند، در نظر داشته باشد. با احتساب ماهیت عمومی و جهانی شبکه‌های اطلاعاتی، یک اقدام بین‌المللی هماهنگ برای رویارویی با چنین سوءاستفاده‌هایی لازم بود. با عنایت به توصیه شماره ۹ (۸۹) که منجر به نزدیکی مفاهیم ملی مرتبط با اشکال خاصی از سوءاستفاده از کامپیوتر می‌شود، نه تنها وجود یک سند بین‌المللی اتصال‌دهنده می‌تواند کارآیی لازم در مبارزه با این پدیده‌های جدید را ایجاد کند، بلکه چارچوب چنین سندی علاوه بر معیارهای همکاری بین‌المللی، باید مسائل مربوط به قوانین آیین دادرسی و اساسی و همچنین موضوعاتی که ارتباط نزدیکی با کاربرد تکنولوژی دارند را مطرح سازد.

۱۰. به‌علاوه کمیته CDPC در گزارشی که به تقاضای خودش توسط «پروفسور کاسپرسن» تهیه شده، به این نتیجه رسیده بود که باید سند قانونی دیگری، مانند کنوانسیون که کارآیی آن از توصیه بیشتر است، ایجاد شود. چنین کنوانسیونی نه تنها باید به مسائل حقوق جزای ماهوی بپردازد، بلکه باید مسائل آیین دادرسی کیفری و همچنین مقررات و توافق‌نامه‌های حقوق جزای بین‌الملل را نیز مدنظر قرار دهد. قبلاً نیز نتیجه مشابه در گزارش ضمیمه توصیه شماره ۹ (۸۹) (R (۲) در ارتباط با حقوق اساسی و توصیه شماره ۱۳، (۹۵) (R (۳) در ارتباط با مشکلات آیین دادرسی مربوط به فناوری اطلاعات را می‌شد، ملاحظه کرد.

1. Cyber Space

حفاظت از سیستم‌های کامپیوتری مستلزم وجود هماهنگی با اقدامات پیشگیرانه و بازدارنـده از رفتار مجرمانه است.

۶. فناوری جدید، مفاهیم قانونی موجود را دچار چالش‌هایی ساخته است. اطلاعات و ارتباطات راه دور به آسان‌ترین وجه در جهان جریان پیدا کرده و مرزها دیگر موانعی بر سر این جریان به‌شمار نمی‌روند. جنایتکاران غالباً در مکان‌هایی به غیر از نقاطی که آثار و نتایج اعمال آنها ظاهر می‌شود، قرار دارند، با این حال کارآیی حقوق داخلی منحصر به قلمرو خاصی است و راه‌حل مشکلات به‌وجود آمده باید توسط حقوق بین‌المللی ارائه شود، که انجام آن مستلزم اتخاذ و به‌کارگیری ابزارهای مناسب حقوق بین‌المللی است. هدف کنوانسیون بوداپست، رویارویی با این چالش و در عین حال احترام به حقوق‌بشر در جامعه اطلاعات نوین، است.

کار مقدماتی

۷. کمیته اروپایی مشکلات جنایی (CDPC) در اجرای مصوبه شماره CDPC/۱۰۳/۲۱۱۱۹۶ در نوامبر ۱۹۹۶ تصمیم به تشکیل کمیته کارشناسان جهت برخورد با جرائم رایانه‌ای گرفت. پایه و اساس تصمیم CDPC توجیهات و استدلالات ذیل است؛

۸. پیشرفت‌های سریع در حوزه فناوری اطلاعات، ارتباط مستقیمی با تمامی بخش‌های جامعه مدرن دارد.

انسجام سیستم‌های اطلاعات و ارتباطات راه دور که صرفنظر از فواصل جغرافیایی کار ذخیره و انتقال تمامی انواع اطلاعات را مقدور ساخته، طیف وسیعی از احتمالات جدید را فراهم کرده است. این پیشرفت‌ها با ظهور شبکه‌ها و ابر شاهراه‌های اطلاعات از جمله اینترنت، گسترش پیدا کرده است که از طریق آنها هر فردی قادر خواهد بود تا به تمامی خدمات اطلاعات الکترونیک[1]، گذشته از اینکه در کدام نقطه این جهان مستقر شده‌اند، دسترسی داشته باشد. کاربران از طریق اتصال به

1. Electronic Information Services

۲. ویژگی برجسته فناوری اطلاعات، تأثیری است که بر تکامل فناوری ارتباطات راه دور گذاشته و خواهد گذارد. ارتباطات کلاسیک همچون انتقال صدای انسان، جای خود را به مبادله مقادیر وسیعی از داده‌ها، صوت، متن، موزیک، تصاویر ثابت و متحرک داده است. این تبادل و تکامل نه تنها بین انسان‌ها بلکه مابین انسان‌ها و کامپیوترها و همچنین بین خود کامپیوترها نیز وجود دارد. اتصالات مداری (Circuit-Switched) جای خود را به شبکه‌های بسته‌ای (Packet-Switched) داده است.

حال دیگر توانایی یا عدم توانایی برقراری یک ارتباط مستقیم چندان حائز اهمیت نیست، بلکه کافی است داده‌ها وارد شبکه‌ای شوند که در آن آدرس فرستنده و مقصد هر فردی که قرار است داده‌ها در اختیار وی قرار گیرد، مشخص باشد تا آنها بتوانند به داده‌ها دسترسی داشته باشند.

۳. استفاده وسیع از پست الکترونیک و دستیابی به اطلاعات از طریق وب سایت‌های متعدد در اینترنت نمونه‌هایی از این پیشرفت‌ها هستند که جامعه را به‌طور پیچیده‌ای دگرگون ساخته‌اند.

۴. سهولت در دسترسی و جست‌وجوی اطلاعات موجود در سیستم‌های کامپیوتری توأم با امکانات عملی نامحدود در مبادله و توزیع اطلاعات، بدون توجه به فواصل جغرافیایی، منجر به رشد سرسام‌آور مقدار اطلاعات موجود و آگاهی که می‌توان از آنها به‌دست آورد، شده است.

۵. این اطلاعات موجب افزایش تغییرات اجتماعی و اقتصادی پیش‌بینی نشده‌ای گردیده است، اما پیشرفت‌های یاد شده حائز جنبه خطرناکی نیز هستند که پیدایش انواع جدید جرائم و همچنین بهره‌برداری از فناوری جدید در ارتکاب جرائم سنتی بخشی از آن به‌شمار می‌رود. به‌علاوه عواقب و پیامدهای رفتار مجرمانه می‌تواند بسیار بیشتر از قبل و دور از تصور باشد، زیرا محدودیت‌های جغرافیایی یا مرزهای ملی آنرا محدود نمی‌کنند. انتشار اخیر ویروس‌های کامپیوتری مخرب در سرتاسر دنیا دلیلی بر این واقعیت است. به‌کارگیری معیارهای حمایت و

ـ کنوانسیون جرائم رایانه‌ای

گزارش توجیهی (تصویب شده در ۸ نوامبر ۲۰۰۱)

این کنوانسیون و گزارش توجیهی آن در یکصد و نهمین اجلاس وزرای شورای اروپا در ۸ نوامبر سال ۲۰۰۱ به تصویب رسید و در تاریخ ۲۳ نوامبر ۲۰۰۱ در کنفرانس بین‌المللی جرائم رایانه‌ای توسط سران کشورها امضا شد.

این گزارش توجیهی تفسیر جامع، کامل و مطمئنی از کنوانسیون مذکور نیست، هر چند ممکن است دارای چنان ماهیتی باشد که بتواند بهره‌برداری از متن کنوانسیون را تسهیل نماید.

مقدمه

۱. انقلاب فناوری اطلاعات به‌طور بنیادین جوامع را دستخوش تغییر و تحول کرده و احتمالاً در آینده قابل پیش‌بینی نیز، این روند ادامه خواهد یافت. انجام بسیاری از مشاغل آسان‌تر شده است. پیش از این فقط روش‌های کار چند بخش خاص از جامعه تحت تأثیر فناوری اطلاعات قرار گرفته بود، اما اکنون به سختی می‌توان بخش‌هایی از جامعه را یافت که تحت تأثیر آن قرار نگرفته باشند. فناوری اطلاعات، تقریباً به نحوی تمام جنبه‌های فعالیت‌های انسان را تحت تأثیر قرار داده است.

ضمائم

پی‌نوشت‌ها:

1. http://www.itiran.com/news/show.asp?no=8210160842
۲. http://www.itiran.com/artic/show.asp?no=8210101026 بـه نقـل از خبرگـزاری فارس‌نیوز
3. http://www.itiran.com/artic/show_user_archive.asp?des=8110&id=17
4. http://www.itiran.com/artic/show_user_archive.asp?des=8204&id=43
5. http://www.itiran.com/artic/show_user_archive.asp?des=8204&id=63
6. http://www.itiran.com/news/show.asp?no=8209041020
7. http://www.itiran.com/artic/show_user_archive.asp?des=8110&id=5
8. http://www.itiran.com/artic/show_user_archive.asp?des=8204&id=32
۹. روزنامه خراسان، سه‌شنبه ۸۲/۱۰/۶، شماره ۱۵۷۴۷، صفحه ۱۰
10. http://www.itiran.com/artic/show_user_archive.asp?des=8106&id=33
۱۱. خبرگزاری دانشجویان ایران، ایسنا، http://www.isna.ir/news/news
12. http://www.itiran.com/artic/show_user_archive.asp?des=8110&id=12
13. http://www.itiran.com/artic/show_user_archive.asp?des=8111&id=9
14. http://www.itiran.com/artic/show_user_archive.asp?des=8202&id=21
۱۵. جنگ اینترنتی ایران و آمریکا، http://ziaiy.persianblog.com، حمید ضیایی‌پرور، وبلاگ خبرنگار

مخدوش خود در منطقه را بهبود بخشد. برمن، رئیس شرکت ضدسانسور آمریکا معتقد است که پراکسی[1] ما به زودی در فهرست سایت‌های ممنوعه قرار خواهد گرفت، اما اگر لازم باشد هر روز از پراکسی جدیدی استفاده خواهیم کرد. وی توضیحی درباره منافع آمریکا از این عمل و باز کردن سایت‌های خلاف اخلاق را نداد. در لایحه‌ای که ماه گذشته به تصویب مجلس نمایندگان آمریکا رسید این‌گونه آمده که دفتری به نام دفتر «آزادی اطلاعات در جهان» ایجاد خواهد شد که با ۵۰ میلیارد دلار بودجه سالانه وظیفه دارد به مردمی که در برخی کشورها با سانسور اینترنت روبرو هستند، کمک کند.

دکتر معتمدی، وزیر پست و تلگراف و تلفن ایران اخیراً در مورد بستن تعدادی از سایت‌های اینترنتی، گفت: «تخلفات اینترنتی، مسئلهٔ روز دنیا است. تفاوتی میان تهمت از جناح راست و جناح چپ نیست و حق شکایت و برخورد وجود دارد. دولت‌ها نیز مکلفند بدون هرگونه جناح‌بندی، طبق قانون از حقوق افراد، سازمان‌ها و ارگان‌ها دفاع کنند.

اصل فیلتر کردن درست است و این مسئله دغدغه تمام خانواده‌ها نیز به‌شمار می‌رود، اما بحث بر سر مصادیق آن است و جایی باید باشد تا این مصادیق تشخیص داده شود که ما مرجع آن نیستیم. یک کمیتهٔ سه نفره توسط شورای عالی انقلاب فرهنگی شامل؛ وزارت ارشاد، اطلاعات و صدا و سیما تشکیل شده است که این مصادیق را بررسی می‌کنند. حدود ۱۷۰ سایت بسته شده‌اند که ۱۶۰ سایت با موضوع ضدانقلاب، ضداخلاقی و توهین به مقدسات بوده است. کمتر از ۱۰ سایت سیاسی نیز بسته شد و طبق گفت‌وگویی که با برخی از گردانندگان آنها داشتیم، خودشان هم به برخی تندروی‌ها و تهمت‌ها اذعان داشتند. ایراد وارده در این میان، آن است که بستن سایت‌ها باید براساس آیین‌نامه‌ای صورت گیرد و کمیتهٔ سه نفره بر این اساس کار کند. این آیین‌نامه در حال آماده شدن است و در صورت تصویب و اجرا، مشکلات به‌وجود آمده نیز حل می‌گردد. برای کار اساسی باید لایحه تخلفات اینترنتی توسط قوه قضائیه تدوین و در دولت تصویب شود و سپس به مجلس رود.(۱۵)

---

1. Proxy

محدوده و اختیارات قانونی یک کشور خارج شده و ابعاد وسیع آن ایجاب می‌کند تا هر کشور قانون مختص به خود را داشته باشد و در ایران نیز لازم است تا برای آگاهی دادن به مردم به‌ویژه قشر جوان نسبت به زیان‌های مالی آن اقدام اساسی، صورت گیرد و قوانینی در منع این عمل وضع شود.

آگاهی مردم

بسیاری از کارشناسان اعتقاد دارند آگاهی مردم همزمان با فعالیت برای ایجاد محدودیت چنین روش‌های بازاریابی ضروری است. به اعتقاد آنان، عامل اصلی در جلب گرایش مردم به سمت چنین تجارت‌های غیرمولدی ناامیدی از کسب درآمد فراوان با افزایش قیمت خدمات عمومی و اجناس است که افراد را به سمت این توسعه پیش می‌برد که می‌توانند با استفاده از چنین روش‌هایی یک شبه ثروتمند شوند.

نصرا... جهانگرد، دبیر شورای عالی اطلاع‌رسانی دراین‌باره گفته است که چنین بازاریابی‌های اینترنتی تقلبی و کلاهبرداری است و باید به مردم آگاهی داد تا فریب این مراکز را نخورند.[۱۴]

۱۵ـ جنگ فیلترها میان ایران و آمریکا

اکنون می‌توان گفت، چالش اینترنتی ایران و آمریکا وارد مرحله تازه‌ای شده که به راحتی می‌توان از اصطلاح «جنگ اینترنتی» برای آن نام برد. چند ماه پس از اجرای سیاست فیلترینگ سایت‌ها در ایران، اینک خبر می‌رسد که «دولت آمریکا با شرکت متخصص شکستن فیلتر و سانسور اینترنت قرارداد بسته، شرکت Anony Mizer از طرف دولت آمریکا مأموریت داشته که اجازه ندهد سانسور در ایران جلوی دسترسی ایرانیان به سایت‌های اینترنتی را بگیرد».

بنا بر گزارش سایت اینترنتی سکیوریتی فوکوس نیوز در این قرارداد، یک پراکسی رایگان برای ایران در نظر گرفته شده که البته این پراکسی، سایت‌های پورنو را فیلتر می‌کند.

آمریکا امیدوار است با کمک به آنچه آن‌را جریان آزادانه اطلاعات می‌خواند، تصویر اخبار

استفاده می‌کردند و با روش‌های مشابهی در اندیشه جذب افراد بیشتری بودند. اخیراً یکی از رسانه‌ها از حضور و ثبت‌نام ۱۸۰ هزار ایرانی تنها در یکی از این شیوه‌های تجارت خبر داد و خاطرنشان کرد که فقط با استفاده از روش‌های پرایم بانک و گلدکوئست بیش از ۲۶ میلیون دلار ارز از کشور خارج شده است.

بنابر گفته منتقدان، اگر پنتاگونو این حسن را داشت که سرمایه در داخل کشور جابه‌جا می‌شد، آن وقت شیوه‌های جدید تقریباً بدون هیچ استثنایی بر خروج سرمایه از کشور تأکید دارند.

فرهاد جواهردشتی، مدیرعامل یک شرکت کامپیوتری در این‌باره به ایسنا گفت: مقدار درآمدهایی که از این طریق از کشور خارج می‌شود، بسیار سنگین است و تأثیر منفی بسیار کلانی بر اقتصاد مملکت می‌گذارد.

آنچه که امروز تحت عنوان تجارت الماس در حال انجام است، در واقع در چارچوب معاملات هرمی قابل تعریف است که از چند سال پیش در برخی از کشورها، قانونی مبنی بر ممنوع شدن آن اعلام گشت، اما این مقوله با تلاش افراد و شرکت‌های مختلف و یافتن راه فرار قانونی مجدداً ادامه یافت.

وی افزود؛ در این نوع بازاریابی که به MULTI-LEVEL MARKETING یا بازاریابی چند سطحی یا هرمی (PYRAMID SELLING) موسوم است به ازای عملی که انجام می‌گیرد، به کسی حقوقی پرداخت نمی‌شود و یک کالا به قیمت بالایی خریداری و افرادی که معمولاً از نظر سطح تحصیلی پایین هستند، سعی می‌کنند تا آن‌را به زیردستان خود به‌صورت درختی به فروش برسانند.

وی تصریح کرد؛ این نوع تجارت در واقع انجام خریدهای بی‌جهتی است که بدون قرعه‌کشی و بدون آنکه چیزی جابه‌جا شود، افراد گاهی به درآمدهایی دست پیدا می‌کنند و در اکثر مواقع سرمایه‌های خود را از دست می‌دهند، بنابراین روش نادرستی است که به‌ندرت منجر به کسب سودی می‌شود که نادرست هم هست.

وی افزود؛ در قدیم این معاملات تنها در یک کشور انجام می‌شد، اما با اینترنتی شدن از

اصفهان، گرگان، شاهرود، سبزوار و ... پرونده‌هایی در همین زمینه وجود دارد نیز این سؤال را پیش آورده که اگر چنین فعالیت‌هایی غیرقانونی است چگونه چند هفته گذشته حداقل ۲ مقاله در حمایت از این تجارت در روزنامه سراسری منتشر شد.

هرچند بنا به گفته یک مقام مسئول که در ارتباط با تخلفات اینترنتی فعالیت دارد یک مرجع قانونی ـ احتمالاً نیروی انتظامی ـ برای آگاه کردن مردم از تخلفات صورت‌گرفته اقدامی را انجام خواهد داد.

خروج ارز از کشور

اساس کار تجارت الماس همچون تجارت باسابقه ـ و البته ممنوع‌شده ـ به نام پنتاگونو است. این روش تجارت که طی زمان کوتاهی جمع وسیعی از ایرانیان را به سمت خود جلب می‌کرد، در ازای بازاریابی و جمع کردن تعداد مشخصی از افراد در این سرمایه‌گذاری، سود مشخصی را برای فرد به همراه می‌آورد. همچنین افراد دیگر نیز به شکلی هرم‌گونه دو گروه از افراد را در دو ستون اطراف خود به چنین کاری وامی‌داشتند. این شیوه در ابتدای ظهور خود تعجب و شگفتی ناظران اقتصادی را برانگیخته بود. چرا که شکل و شیوه اقتصادی به کار رفته در آن از بیرون نادرست به‌نظر نمی‌رسید.

پنتاگونو خیلی سریع به شکل‌های دیگری نیز تقسیم شد، اما پس از غیرقانونی اعلام شدن، ناگهان بساط آن برچیده شد. در این میان، افرادی که در هفته‌های آخر به سرمایه‌گذاری در آن پرداخته بودند و از قضا تعداد زیادی را نیز تشکیل می‌داد، ضرر کردند و در مقابل، سردمداران این تجارت به پول‌های کلانی دست یافتند. نقطه ضعف پنتاگونو این بود که صاحبان آن مجبور بودند برای بازاریابی و نقل و انتقالات مالی یک محل فیزیکی را در نظر بگیرند، اما فرزندان پنتاگونو که مانند تمام بچه‌های امروزی به کامپیوتر و اینترنت مجهز بودند از این امکان به خوبی استفاده کردند و فضای آزادانهٔ شبکه اقدامات و فعالیت‌های خود را گسترش دادند. کیمبرلی سولاتیر، پرایم بانک، گلدکوئست و مای سون دایاموند همه به نوعی از اینترنت

خود و سایر جوانان را که آینده‌سازان این مرزوبوم هستند، برای درآمدهای زودگذر و واهی خواهید گرفت؟ آیا به فکر اعتبار شخصی خود نیستید که پس از فروپاشی این شبکه، نسبت به اقوام و دوستان نزدیک خود چقدر خجالت‌زده خواهید شد؟

۱۵. آیا شما تجارت شبکه‌ای می‌شناسید که بیش از ۵ سال سابقه و عمر داشته و یا توانسته باشد که عمر کرده و فعال بماند؟ آیا از اهداف گردانندگان اصلی این شبکه‌ها مطلع هستید؟ آیا شما به‌عنوان یک ایرانی باید به فکر رشد و ترقی مملکت و میهن خودتان باشید و یا اینکه در جست‌وجو چند صد دلار و یک زندگی مرفه رؤیایی، وقت خود و دیگران را از بین برده و حتی آبرو و اعتبار خود را در گرو این کار بگذارید؟

احساس می‌کنیم که ۱۵ سؤال گذشته به‌قدر کافی ذهن شما را فعال نموده تا قدری منطقی‌تر فکر کنید و از ادامه این‌گونه فعالیت‌ها بپرهیزید. مطمئناً به زودی قوانین لازمه جهت برخورد قانونی با فعالان چنین شبکه‌هایی تبیین خواهند شد و امیدواریم شما دوست گرامی جزو آن دسته افرادی نباشید که جهت کسب درآمد، خود و دیگران را در یک چاه تاریک گمراهی گرفتار نموده باشید. به زودی اطلاعات تکمیلی بیشتری از نحوه فعالیت‌های شبکه‌های مشابه در اختیار هموطنان قرار خواهد گرفت.[۱۳]

۱۴ـ فرزندان پنتاگونو

ـ تجارت الماس توسط اینترنت اکنون به بحث روز تبدیل شده و بسیاری از کارشناسان به اظهارنظر دراین‌باره می‌پردازند و حتی موضوع تا آنجا پیش رفته که دبیر شورای عالی اطلاع‌رسانی نیز در این مورد به موضع‌گیری پرداخته است.

شاید تا چندی قبل کمتر کسی با نام تجارت الماس آشنا بود، اما پس از انتشار یک سلسله مقاله، مصاحبه و گزارش در این‌باره در مطبوعات، اکنون وضعیت متفاوت شده است.

از سوی دیگر، اعلام این خبر که حدود ۱۸۰ هزار ایرانی به این نوع تجارت آلوده شده‌اند نیز بر بهت و حیرت‌ها در این زمینه افزود هر چند اعلام این خبر که در شعبه دادگاه‌های

۵. آیا می‌دانید که شرکت‌های بزرگ و عظیم همیشه از Network Solutions جهت ثبت دامین استفاده می‌کنند تا ثبت‌کننده اصلی دامین را به نام خود معرفی نمایند؟ چرا این شرکت یک دامین ۸ دلاری از یک شرکت چینی تهیه کرده است؟

۶. آیا دقت کرده‌اید که طراحی سایت به صورت کاملاً غیرحرفه‌ای انجام شده است؟ حتی تصاویر پس‌زمینه به صورت غلط و نامرتب چیده شده که معمولاً یک طراح حرفه‌ای چنین ایرادهایی ندارد؟ آیا شما به‌عنوان دارنده یک شبکه مولتی میلیونری، نتوانسته‌اید ۳۰۰ دلار برای یک طراحی شکیل و زیبا بپردازید؟

۷. آیا دقت کرده‌اید که تنها در بخش فروشندگان شماره تلفن برای کشورهای ایران، امارات و پاکستان داده شده است؟ جالب‌تر اینکه برای فنلاند هم شماره تلفن داده شده، اما شماره تلفن غلط است و وجود خارجی ندارد؟

۸. آیا می‌دانید که این شرکت از آرم بانک ملی به‌عنوان بانک همکار استفاده می‌کند در حالی که مسئولان بانک این همکاری را کاملاً رد کرده‌اند؟

۹. آیا می‌دانید چک‌های بانک سیبا که توسط کامپیوتر بازسازی و چاپ شده است، در اختیار افراد زیادی جهت جلب اعتماد مردم دست به دست می‌شود؟

۱۰. آیا می‌دانید که شایعاتی همچون کمک‌های این شرکت به فلسطینی‌ها و یا کمک‌های انسان‌دوستانه دیگر چقدر ساده‌لوحانه، مردم مملکت ما را فریب می‌دهد؟

۱۱. آیا می‌دانید اگر شما و یا دوستانتان مبالغی را به‌عنوان سود دریافت کرده‌اید، تنها نیت این شرکت جلب اعتماد شما و فعال‌تر کردن شما بوده است؟

۱۲. آیا تاکنون جست‌وجو کرده‌اید که ببینید صدها سایت اینترنتی چنین تجارت‌های شبکه‌ای انجام می‌دهند؟

۱۳. به‌نظر شما سابقه ۱۹۳۷ مسئول اصلی شرکت که در سایت قید شده صحیح است یا علامت Copyright 1979 و یا ثبت شرکت در سال ۲۰۰۲میلادی؟

۱۴. آیا شما به‌عنوان یک خریدار و عضو فعال این شبکه، آن‌قدر متعصب شده‌اید که وقت

شبکه‌ای چه تجربیات تلخی را به‌جای گذاشت؟ آیا می‌دانید حضور کشور آلبانی بر روی نقشه جغرافیایی کره زمین به چه دلیل دچار تردید گشته است؟

آیا می‌دانید این‌گونه شبکه‌ها در هزاره جدید تنها در کشورهای جهان سوم و به‌خصوص در منطقه خاورمیانه ۹۰ درصد فعالیت دارند. کشورهایی همچون ایران، امارات، پاکستان، بحرین، هند و تا حدی ترکیه، از کشورهای فعال در این زمینه هستند؟ آیا مردمان غرب آن‌قدر نادان هستند که ارزش تجارت شبکه‌ای را درک نمی‌کنند و یا تجربیات و دانشی دارند که مردمان ما لز آن بی‌بهره هستند. در سال ۱۳۸۲ شرکتی با نام شرکت «پرایم بانک» در شهرهای اصفهان، تهران و مشهد فعالیت‌هایی را از خود نشان داده و مطابق با بررسی‌های انجام‌گرفته، جوانان بسیاری نیز در این شبکه فعال شدند. در اینجا لازم است نکات مهمی را مدنظر قرار دهید تا شما نیز از محتوای اصلی این‌گونه شبکه‌ها مطلع شوید. این شرکت حتی مبالغی را از طریق نمایندگان خود در ایران و یا به‌صورت شبکه به فعالان شبکه پرداخت کرده تا از این طریق اطمینان افراد را به خود جلب نماید. به همین دلیل سعی داریم چند سؤال مهم در اینجا مطرح کنیم تا ذهن پویای شما، به‌دنبال پاسخ مثبت برای آن باشد.

۱. آیا شما شرکت پرایم بانک را به‌عنوان یک بانک خصوصی که در ایالات‌متحده فعال است، می‌شناسید؟ (در این زمینه به آدرس http://www.primebank.com مراجعه کنید.)

۲. آیا متوجه شده‌اید که پرایم بانک جدید، یک Ltd اضافه دارد؟ آیا می‌دانید که تنها com. برای این دامین ثبت شده و آن هم در ماه جولای سال ۲۰۰۲ یعنی درست چند ماه پیش؟

۳. آیا می‌دانید تمام شرکت‌های بزرگ، معمولاً تمام پسوندهای دامین را با آرم Trade Mark به نام خود می‌کنند؟ چطور یک شرکت بزرگ حتی هزینه چند دلاری برای ثبت چند دامین کناری خود را هم نداشته است؟

۴. آیا می‌دانید که شرکت پرایم بانک به نام یک شرکت با مسئولیت محدود، درست ۵ روز پس از ثبت دامین خود در تاریخ ۲۰۰۲/۸/۱ در کشور انگلیس با شماره SC234860 ثبت شده است؟

در سال ۱۳۸۲، تجارت شبکه‌ای[1] به‌طور محسوسی در ایران باب شد و متأسفانه به‌رغم تجربیات تلخ گذشته، همچنان می‌بینیم که افراد بسیاری وارد این شبکه‌ها شده و اقدام به فعالیت می‌نمایند. اصولاً صاحبان اصلی یک شبکه، برای جذب طرفداران بیشتر، اقدام به تبلیغات وسیع در محدوده‌های خاص جغرافیایی می‌کنند و با دادن فرمول‌های مختلف شبکه (مانند ۵ تا چپ ۵ تا راست) مردم را نسبت به سودهای آنچنانی ترغیب می‌کنند. جالب‌تر آنکه بدانید این‌گونه شبکه‌ها بسته به قدرت و نفوذ صاحبان اصلی تا مدت مدیدی همچون ۶ ماه یا یک‌سال و حتی ۲ سال، اقدام به رعایت فرمول خود می‌کنند. بدین‌گونه که سودهایی را به افراد فعال در شبکه خود پرداخت می‌نمایند و حتی حضور سکه‌های طلا، الماس، چک‌های خارجی، چک‌های بانک‌های داخلی و حتی پول نقد در حساب بانکی افراد، به آنها اطمینان می‌دهد که این‌گونه شبکه‌ها واقعاً سودده و کارآمد هستند و جای هیچ‌گونه ابهامی ندارند. مواقعی که از افراد فعال در این شبکه‌ها بپرسند که این سود در برابر چیست، پاسخ می‌دهند: در برابر زحمت بازاریابی هر قدرت بیشتر فعالیت کنی، بیشتر سود می‌کنی؟ آیا به‌نظر شما ترغیب دیگران به خرید و شرکت در این شبکه‌ها و همچنین آوردن رقم‌های بزرگ در ذهن افراد و به تصویر کشیدن یک زندگی مرفه و بی دردسر و حتی دادن وعده‌های آنچنانی که خود شما هم آنچنان به اصل و نسب آن مطمئن نیستید، یک درآمد آبرومندانه و عاقلانه است؟ آیا می‌دانید حضور این‌گونه شبکه‌ها چه ضربه محکمی به روال فعالیت‌های علمی و روند توسعه تکنولوژیکی کشور ایران خواهد زد؟

چه بسیار نوجوانانی را می‌بینیم که به‌جای تحصیل علم، تکنیک و تجربه، شروع به بازاریابی در این شبکه‌ها می‌کنند و ساعت‌ها وقت خود را برای ترغیب دیگران صرف می‌کنند و حتی این کار را جزو افتخارات خود محسوب می‌کنند. تا چه زمان کشور و مردمان ما باید در این تلاطم جهل و نادرستی که ریشه‌ای جز ساده‌انگاری و جاه‌طلبی نسبی ندارد، غوطه‌ور باشند؟ آیا می‌دانید در کشورهای غربی در بین سال‌های ۱۹۹۵ تا ۱۹۹۹ میلادی، تجارت

1. Network Marketing

انتظامی واحد خاصی را برای مبارزه با جرائم کامپیوتری ایجاد کرده، اما مشکل نیروی انتظامی آن است که در پرونده‌های کلانتری‌ها، این جرائم با عنوان جرائم بی‌اهمیت دسته‌بندی شده و تاکنون، نیروی انتظامی توجهی به رسیدگی تخصصی به این پرونده‌ها نداشته است.

نگرانی آینده

دشوار می‌توان به شرح این دنیای گسترده پرداخت. هنگامی‌که یک انسان ضعیف از لحاظ مالی و جسمی می‌تواند میلیون‌ها انسان دیگر را در مدت کوتاهی غافلگیر کند و سرنوشت آنان را تغییر دهد، این عمل بیشتر به اقدامی خارق‌العاده یا وقایع نادر طبیعت شباهت دارد. این پرسش هنوز ذهن بسیاری را به خود مشغول کرده است که اگر یک کاربر به یکی از پایگاه‌های حیاتی کشور، نظیر کنترل پرواز فرودگاه، برنامه رزرو بلیت مسافران، نتایج کنکور سراسری، پرونده افراد در تأمین اجتماعی، مرکز کنترل ترافیک، پایگاه ثبت احوال، بانک مرکزی و سازمان مدیریت و برنامه‌ریزی نفوذ کند، این مراکز تا چه میزانی آمادگی برخورد با آنسرا خواهند داشت؟ با وجود مشکلات مطرح شده، این سؤال مطرح است که اگر مقامات انتظامی موفق به کشف و شناسایی فرد خاطی شوند، سازوکار مناسب به‌منظور اثبات جرم و تنظیم مستندات قابل ارائه در محاکم قضایی کدام است و سازمان رسیدگی‌کننده به این‌گونه جرائم مجازی و الکترونیکی دارای چه ویژگی‌هایی خواهد بود؟[۱۲]

۱۳ـ تجارت شبکه‌ای در ایران و مفاسد آن

طی سال‌های اخیر شاهد ظهور قارچ‌گونه شرکت‌ها و مؤسسات مالی و تجاری مجازی در اینترنت هستیم. متأسفانه به‌دلیل اینکه اغلب کاربران ایرانی نسبت به این جامعه مجازی، ناآشنا هستند، توسط تبلیغات سوء و هدفمند شرکت‌های داخلی و خارجی گمراه شده و مسیرهای ناآزموده‌ای را طی می‌کنند.

فرد دیگری را فریب دهد. اما وقتی فردی، با سوءاستفاده و دستکاری در سیستم بانکی، مبالغ کلانی را تصاحب می‌کند بدون اینکه انسانی را فریفته باشد، از چه قانونی می‌توان برای مجازات وی کمک گرفت؟

در اینجا نحوه ارتکاب جرم با گذشته یکسان نیست، از این‌رو ماده قانونی مربوط به کلاهبرداری که در تعریف دوم تأکید دارد که «هرکسی دیگری را بفریبد» کلاهبردار است، کارآیی خود را از دست می‌دهد.

بسیاری از اشکالات از آنجا ناشی شده است که حقوق جزا در ایران به حمایت از اشیا، موضوعات و اهداف مادی ملموس و فیزیکی پرداخته و از اشیا، موضوعات و اهداف ملموس و غیرفیزیکی کمابیش غافل مانده است.

این سؤال مطرح است که در یک «محیط دیجیتال»[1] چه چیز قابل توقیف است؟ آیا داده‌ها را می‌توان توقیف کرد؟ آیا ذخیره‌سازی و ارائه داده‌ها و اطلاعات را می‌توان به‌عنوان اشیا موضوع توقیف، همچون موارد فیزیکی، تحت شمول قوانین دادرسی قرار داد؟

نقش نیروی انتظامی

سؤالات بسیاری در این زمینه وجود دارد که قوانین ایران تا حد زیادی درباره آنها سکوت کرده است. اما مسئله تنها به مشکلات موجود در زمینه جرائم کامپیوتری مربوط نمی‌شود.

مقامات انتظامی هم در این زمینه سؤالاتی دارند که نمی‌توان آنها را نادیده گرفت. آنان می‌گویند، آیا افسران پلیس می‌توانند به‌عنوان یک کاربر در اینترنت به جست‌وجو بپردازند و اطلاعات کشف‌شده را ضبط و علیه متهم در دادگاه از آنها استفاده کنند؟

قوانین ایران در این زمینه پاسخی ندارد و نه تنها پلیس چنین اجازه‌ای را ندارد، که حتی در صورت دسترسی به اطلاعات نیز نمی‌تواند از آن به‌عنوان ادله علیه مجرم استفاده کند. نیروی

---

1. Digital Environmet

مأموران تاکنون چنین آموزش‌هایی کسب کرده و یا حتی میزان آموزش آنها کافی بوده باشد.

ضعف قوانین

نبود قوانین و مقررات در این زمینه از جمله مشکلات قضایی و انتظامی ایران است. اولین قانون مصوب در زمینه حقوق مالکیت فکری در ایران در سال ۱۳۱۰ تدوین شد و حدود چهل سال بعد، قانون حمایت از حقوق مؤلفان و مصنفان در سال ۱۳۴۸ به تصویب رسید.

گزارش‌ها نشان می‌دهد که آرای قضایی صادرشده در این زمینه یا بسیار کم بوده یا در برخی جنبه‌ها، به‌هیچ‌عنوان وجود نداشته است. به‌جز این، بعد از انقلاب نیز موضوع حمایت از مؤلفان و مصنفان زیر سؤال رفت و سیستم قضایی نیز از قوانین موجود استفاده‌ای به‌عمل نیاورد.

قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای کامپیوتری، که در ۱۰ دی‌ماه سال ۱۳۷۹ به تصویب رسید، اگرچه مورد استناد دادگاه‌هاست، اما نواقصی چون نداشتن آیین‌نامه اجرایی، مشکلاتی را در اجرای این قانون به همراه داشته است.

هر روز بر تعداد کامپیوترها افزوده می‌شود و از همین رو باید در انتظار وقوع گسترده‌تر جرائم نیز بود. گستردگی کار سبب شده تا کشورهای دیگر برای جرائم کامپیوتری، دسته‌بندی‌های خاصی را منظور کنند، اما در ایران این مشکل هنوز حل نشده و قوانین جزایی از قوام و وسعت لازم برای برخورد با این جرائم برخوردار نیستند.

کارشناسان معتقدند جرم کامپیوتری، موجب تغییر در اجزای عنصر مادی و بعضاً معنوی جرم شده و از این‌رو، اساس اقدام مجرمانه را تغییر داده است.

کدام تعریف؟

این کارشناسان می‌گویند در جرم کلاهبرداری، لازم است فرد خاطی با انجام ترفندهایی،

پورتلند، اورگان

آتلانتا، جرجیا

جلسات عمومی برنامه‌ریزی‌شده برای آینده عبارتند از؛

سن‌آنتونیو، تگزاس

فیلادلفیا، پنسیلوانیا

بوستون، ماساچوست

پیتس بورگ، پنسیلوانیا

نیویورک سیتی، نیویورک

فونیکس، آریزونا

سن‌دیگو، کالیفرنیا

هیأت «حفاظت زیرساخت حیاتی» ریاست‌جمهوری

پس از بررسی که در ابتدای دولت بوش صورت گرفت، رئیس‌جمهور فرمان اجرایی ۱۳۲۳۱ (حفاظت زیرساخت حیاتی در عصر اطلاعات) را در اکتبر ۲۰۰۱ امضا کرد و «هیأت حفاظت زیرساخت حیاتی» ریاست جمهوری را تأسیس نمود. این هیأت، مرکز امنیت اینترنتی[1] در قوه مجریه و متشکل از مقامات ارشد بیش از ۲۰ وزارتخانه و ارگان است. رئیس‌جمهور یک‌سری کمیته‌های بین ارگانی را ایجاد کرد که درباره مسائلی از قبیل آموزش و پرورش، تحقیقات، عکس‌العمل شرایط اضطراری و مسائل وابسته آن به هیأت مزبور گزارش می‌دهند.

برخی قسمت‌های این استراتژی، مفصل‌تر از سایر بخش‌هاست. اما با تکامل استراتژی در نگارش‌های بعدی، سعی خواهیم داشت به کلیه مسائل عمده امنیت اینترنتی با جزئیات کافی بپردازیم. این استراتژی حکم نقشه راهنما برای دولت، کنگره، دولت‌های ایالتی و محلی، بخش‌های مختلف اقتصاد، آموزش عالی و کاربران آمریکایی اینترنت را دارد.

---

1. Central for Internet Security

توصیه‌ها برای اقشار مختلف مخاطبان از جمله خود دولت ارائه می‌شوند. این استراتژی جایگزینی برای فرآیند عادی تصمیم‌گیری درباره بودجه و سیاست‌ها نیست. در عین حالی که بسیاری از توصیه‌های ارائه‌شده در استراتژی حاضر، نیازمند منابع و امکانات اضافی نیست، اما توصیه‌هایی که به منابع اضافی نیاز داشته باشند در فرآیندهای عادی مورد بررسی و رسیدگی قرار خواهند گرفت. بسیاری از توصیه‌ها در دستور کار «هیأت حفاظت زیرساخت‌های حیاتی» و کمیسیون‌های بین سازمانی آن قرار خواهند گرفت.

نگارش بعدی این استراتژی منعکس‌کننده تصمیمات اتخاذشده در فرآیند تنظیم بودجه سال ۲۰۰۴ و اقدامات هیأت یادشده و کمیسیون‌های آن و همچنین پیشرفت‌های وزارتخانه‌ها و ارگان‌های مختلف خواهد بود.

استراتژی برای اینترنت در اینترنت

نسخه چاپی این سند به مکان‌هایی بر روی اینترنت اشاره دارد که استراتژی‌های تهیه‌شده توسط گروه‌های مختلف و همچنین سایر مطالب مفید قرار دارند. به‌علت محدودیت جا، نسخه چاپی شامل متن مراجع نیست. اما در نسخه برخط (Online)، پیوندهای فرامتنی (Hyperlink) به این مراجع وجود دارد. در این سند، اجزای اصلی استراتژی یادشده آمده است؛

- خط مشی: تهدیدها و نقاط ضعف اینترنت
- سیاست‌ها و اصول راهنمای استراتژی
- نکات اصلی استراتژی
- پنج سطح «استراتژی ملی» (کاربر خانگی، شرکت‌های بزرگ، شرکت‌های کوچک، بخش‌های حیاتی کشور و جامعه جهانی). در هر پنج سطح نسخهٔ برخط، کادرهای برنامه کاری به‌صورت سایه‌دار مشخص می‌شود.

در نسخه کاغذی، «توصیه‌ها، برنامه‌ها و مباحث» به‌طور خلاصه در پایان هر سطح می‌آید.

در نهایت با گذشت زمان «مباحث» باید منجر به «توصیه» شده یا بدون نتیجه خاتمه یابند. «توصیه‌ها» هم به همین ترتیب تکامل می‌یابند. «توصیه‌ها» در برخی موارد، مبدل به طرح‌های سازمان‌های خصوصی یا طرح‌های شخصی شده و در سایر موارد توسط دولت دنبال می‌شوند. به‌علت ماهیت متغیر اینترنت، ممکن است با بررسی دقیق‌تر تشخیص داده شود که برخی توصیه‌ها امکان‌پذیر یا مقرون به صرفه نیستند. نگارش‌های بعدی استراتژی ملی اطلاعات به‌هنگام در مورد این نتایج را بیان خواهد کرد. استراتژی حاضر دارای پیوندهای فرامتنی[1] به اسناد و صفحات وب[2] سازمان‌های غیردولتی، مجامع تجاری، مؤسسات آموزش عالی، دولت‌های محلی و ایالتی و شرکت‌ها است. محتوای این اسناد و صفحات تنها توسط مؤسسات مربوطه تعیین شده و شمول این مطالب در اینجا به معنی پذیرش دیدگاه‌های آنان از سوی دولت فدرال نیست، دلیل گنجاندن این مطالب آن است که استراتژی ملی، نسخه تجویزی دولت فدرال نیست، بلکه قصد بر آن است که فرآیند تدوین استراتژی به‌صورت مشارکتی صورت گیرد.

لطفاً با پیوستن به این فرآیند به تأمین امنیت اینترنت کمک کنید تا ایالات متحده بتواند همچنان از مزایای «انقلاب فناوری اطلاعات» در آموزش و پرورش، بهداشت و علوم پزشکی، اقتصاد، دولت الکترونیک و دفاع ملی بهره‌مند شود. تنها با حفظ امنیت اینترنت است که می‌توان از مزایای بعدی اینترنت به‌طور کامل بهره گرفت.

تهدیدات و آسیب‌پذیری‌های اینترنت؛ خط‌مشی اجرایی

یک هفته پس از حملات ۱۱ سپتامبر، حمله دیگری به شرکت‌های خدمات مالی که فاصله چندانی با محل مرکز تجارت جهانی نداشتند، صورت گرفت. حمله‌ای با تخریب فیزیکی کمتر، اما با اهمیت اقتصادی فراوان. اهمیت آن در خسارت مالی قابل ملاحظه ایجاد شده، نبود بلکه این حمله هشداری بود از آنچه ممکن است در آینده رخ دهد. نام این حمله (NIMDA

---

1. Hyperlinks

2. Docummment and Page web

کلمه ADMIN با املای برعکس) بود و برای ملتی که به شبکه‌های کامپیوتری وابسته شده، هشداری بیدارکننده بود. NIMDA یک حمله اینترنتی خودکار بود؛ آمیخته‌ای از یک کرم کامپیوتری (WORM) و یک ویروس کامپیوتری که با سرعت وحشتناکی در سراسر کشور منتشر می‌گشت و از راه‌های مختلفی برای آلوده کردن سیستم‌های کامپیوتری وارد می‌شد. آلوده شدن کامپیوتر به معنای نابودی فایل‌های آن بود. این حمله در عرض یک ساعت به بلایی همگانی مبدل شد که چندین روز به طول انجامید و به ۸۶۰۰۰ کامپیوتر حمله کرد.

NIMDA مشکلات فراوانی در صنایع امنیتی ایجاد کرد. شرکت‌ها، بخش برخط (Online) خود را تعطیل کردند، دسترسی مشتریان به خدمات برخط قطع شد و حتی برخی شرکت‌ها مجبور شدند سیستم‌هایشان را دوباره به‌طور کامل بسازند. هزینه مالی واقعی حمله NIMDA مشخص نیست، زیرا روش همسانی برای ارزیابی این خسارات وجود ندارد. اما منابع موثق صنعتی، هزینه مالی حملات اینترنتی ناشی از کدهای آلوده را در سال ۲۰۰۱، ۱۳ میلیارد دلار برآورد کرده‌اند. دو ماه قبل از حمله NIMDA، حمله اینترنتی به نام (Code Red رمز قرمز)، ۱۵۰۰۰۰ سیستم کامپیوتری را در عرض ۱۴ ساعت آلوده کرد و موجب میلیاردها دلار خسارت شد. این حملات، نمایانگر رشد قدرت تخریب و پیچیدگی حملات اینترنتی است. حجم این قبیل حملات هم قابل ملاحظه می‌باشد. مرکز هماهنگی «بخش عکس‌العمل‌های اضطراری شبکه‌های کامپیوتری (CERT)» دانشگاه Carnegie Mellon در سال ۱۹۹۸، ۳۷۰۰ مورد حمله را گزارش داد و با نرخ‌های فعلی، بالغ بر ۱۱۰۰۰۰ فقره حمله را در سال ۲۰۰۲ گزارش خواهد داد. سایر گروه‌ها رشد مشابه وحشتناکی در حملات کامپیوتری را گزارش دادند که احتمالاً این روند ادامه خواهد یافت.

ملتی کاملاً وابسته به اینترنت

«انقلاب فناوری اطلاعات» روش عملکرد و خدمات‌دهی شرکت‌ها و دولت در ایالات‌متحده را بی‌سروصدا تغییر داد. کشور ما بدون تأمل کافی درباره امنیت، کنترل

فرآیندهای کلیدی در تولید، تسهیلات، بانکداری و مخابرات را به شبکه‌های کامپیوتری محول کرد. در نتیجه، هزینه‌های کاری تنزل یافت و بهره‌وری چندین برابر شد. این روش همچنان در جهت استفاده بیشتر از سیستم‌های شبکه کامپیوتری ادامه دارد.

در حال حاضر (سال ۲۰۰۲) اقتصاد و امنیت ملی ما کاملاً وابسته به فناوری اطلاعات و زیرساخت اطلاعاتی است. شبکه‌ای از شبکه‌ها عملیات تمامی بخش‌های اقتصاد ما اعم از انرژی (برق، نفت و گاز)، حمل‌ونقل، بهداشت، خدمات اضطراری، آب، صنایع شیمیایی، صنایع دفاعی، فرآورده‌های غذایی، کشاورزی و پست را به‌طور مستقیم کنترل و پشتیبانی می‌کند.

حوزه این شبکه‌های کامپیوتری از مرزهای فضای مجازی هم فراتر می‌رود. این شبکه‌ها همچنین تجهیزات فیزیکی از قبیل ترانسفورماتورهای برق، قطارها، پمپ‌های خط لوله، مخازن شیمیایی، رادارها و بازارهای بورس را کنترل می‌کنند. محور اصلی زیرساخت اطلاعاتی که ما به آن وابسته هستیم، اینترنت است. سیستمی که در ابتدا برای تبادل اطلاعات غیرسری بین دانشمندان طراحی شد و البته فرض بر آن بود که این افراد علاقه‌ای به سوءاستفاده از این شبکه ندارند. همین اینترنت، امروزه میلیون‌ها شبکه کامپیوتری را به یکدیگر متصل می‌کند و شبکه‌ها هم بخش عمده خدمات حیاتی کشور را تأمین می‌کنند. همراه با رشد فزاینده و حیرت‌انگیز اینترنت در جهان، امنیت آن هم پیوسته تنزل یافته است. افراد تقریباً از هر کشوری بر روی کره زمین به این شبکه دسترسی دارند و این شبکه هم به نوبه خود به شبکه‌های اداره‌کننده خدمات حیاتی در ایالات متحده متصل است.

حملات اینترنتی به شبکه‌های اینترنتی ایالات متحده به‌طور مرتب رخ می‌دهد و می‌تواند نتایجی وخیم همچون مختل کردن عملیات حیاتی، از دست رفتن درآمدها و دارایی‌های فکری و خسارات جانی به‌دنبال داشته باشد. مقابله با چنین حملاتی مستلزم توسعه قابلیت‌های ویژه در مکان‌هایی است که امروزه فقدان آنها احساس می‌شود و این در کاهش نقاط ضعف، شناسایی و بازداشتن افراد و سازمان‌های دارای این قابلیت‌ها و اهداف خرابکارانه علیه زیرساخت‌های ملی، ضروری است.

حوزه‌های تهدیدات

گروهی از مهاجمان به زیرساخت اطلاعاتی حمله می‌کنند. این مهاجمان شامل؛ اسکریپت‌بازها (Script Kiddies) که نرم‌افزارهای مخرب را از اینترنت به‌منظور انجام حملات اینترنتی مخرب و آزاردهنده شعارنویسی (Graffiti) مشابه می‌گیرند، هکرهایی که صرفاً قصد نمایش دادن مهارت‌های ویران‌کننده خود را دارند، عوامل خودی مورد اطمینان که از دسترسی خود به سیستم‌های کامپیوتری برای صدمه زدن به سازمان‌های جنایتکار مشغول به کلاهبرداری، اخاذی و سرقت اینترنتی، استفاده می‌کنند، سازمان‌های جنایتکاری که از طریق اینترنت دست به دزدی، کلاهبرداری و اخاذی می‌زنند و یا تروریست‌ها و سازمان‌های دولتی دشمن که اکنون جاسوسی ما را می‌کنند، می‌شوند. آنها مشغول تهیه برنامه‌هایی برای صدمه‌زدن به اقتصاد ما و تضعیف یا به‌دست گرفتن کنترل سیستم‌های فیزیکی و اینترنتی در نبردهای آینده با ایالات‌متحده هستند و اینجاست که ایالات‌متحده باید به مقابله با این مهاجمان بپردازد.

شناسایی افرادی که حمله کرده‌اند و یا ممکن است حمله کنند، نه تنها فرصتی را برای بازداشتن و محاکمه کردن آنان (برای مثال دستگیری جنایتکاران یا توسل به نیروی نظامی در حملات از نوع جنگ اطلاعات) فراهم می‌کند، بلکه باعث می‌شود تا ما سلسله مهارت‌های آنان را آموخته و بهتر بر روی برنامه‌های حفاظت ملی متمرکز شویم.

کاهش نقاط آسیب‌پذیر در حالتی که تهدیدهای شناخته‌شده وجود ندارد.

در عین حال که کشور باید به تهدیدات مشخص بپردازد، به تأخیر انداختن رفع کوچک‌ترین نقص جدی در زیرساخت‌های حیاتی به زمانی‌که از یک حمله قریب‌الوقوع توسط مهاجمی خاص باخبر شویم، استراتژی بسیار خطرناکی برای قربانیان احتمالی به‌شمار می‌رود.

هر دو حملهٔ اینترنتی کد قرمز و نیمدا (NIMDA) در سال ۲۰۰۱، بدون هیچ‌گونه اعلان خطری به شبکه‌های کشور راه یافتند و چنان سریع منتشر شدند که بسیاری از قربانیان فرصتی

برای آگاه شدن از خطر حمله نیافتند و حتی اگر هم داشتند بسیاری از آنها وقت، اطلاعات یا ابزارهای حفاظت از خود را در اختیار نداشتند. احتمالاً ایجاد سد دفاعی در برابر چنین حملاتی در برخی موارد چندین روز به طول می‌انجامید.

بررسی سناریوی زیر ...

یک روز صبح ارگانی تروریستی اعلام می‌کند که شبکه برق شمال‌غربی اقیانوس آرام را به مدت ۶ ساعت از ۴ بعدازظهر قطع خواهند کرد و همین کار را هم اجرا می‌کنند. سپس همان گروه اعلام می‌کند که مدارهای اصلی مخابرات بین شرق و غرب ایالات‌متحده را به مدت نصف روز از کار خواهد انداخت و این کار را هم به‌رغم کوشش‌های ما جهت مبارزه علیه آنها انجام می‌دهند. سپس این گروه تهدید می‌کند که سیستم کنترل ترافیک هوایی شهر نیویورک را از کار انداخته، مانع پروازها شده و مسیر پروازهای داخلی را منحرف می‌سازد و این کار را هم انجام می‌دهد. تهدیدات به‌طور پیاپی ادامه یافته و با موفقیت اجرا می‌شوند که این امر نمایانگر توانایی دشمن برای حمله به زیرساخت‌های حیاتی ماست.

در نهایت آنها تهدید می‌کنند که اگر لیست خواسته‌هایشان برآورده نشود، تجارت الکترونیک و سرویس کارت اعتباری را به‌وسیله چندصد هزار هویت ربوده‌شده در میلیون‌ها معامله تقلبی، از کار خواهند انداخت. بنابراین هراس، آشوب و اغتشاش عمومی پس از این تهدید را تجسم کنید. آنچه که باعث می‌شود این سناریو جالب و هشداردهنده تلقی شود آن است که حوادث فوق‌الذکر قبلاً اتفاق افتاده‌اند، اما نه به‌طور همزمان و نه با مقاصد تخریبی، بلکه همگی به‌صورت حوادث تکی و انفرادی به مرور زمان روی دادند؛ برخی در خلال خرابی‌های فنی، برخی در مانورهای تمرینی ساده و برخی در حملات واقعی اینترنتی. به هر حال مسئله قابل توجه این است که تمامی این حملات به‌وسیله حملات اینترنتی از راه دور قابل اجرا هستند.

خلاصهٔ نامه‌ای به رئیس‌جمهور از سوی ۵۰ دانشمند، متخصص کامپیوتر و مأموران سابق اطلاعات

درس مهمی که از این حملات اینترنتی و امثال آنها باید آموخت این است که افراد متکی به سیستم‌های کامپیوتری شبکه‌ای، لازم است نقاط آسیب‌پذیری خود را هم‌اکنون شناخته و نسبت به رفع آنها اقدام کنند، نه اینکه منتظر بمانند تا جلوی تهاجم از جای دیگری گرفته شود و یا خبر یک حمله قریب‌الوقوع به آنها داده شود. تاکنون هیچ‌کس به‌خاطر حملات نیمدا و کد قرمز دستگیر نشده است. به هر حال لازم به ذکر است که حملات کامپیوتری جرائم جدی هستند و تعداد افرادی که به این دلیل دستگیر می‌شوند رو به افزایش است.

شناسایی نقاط ضعف از طریق اجرای ممیزی امنیتی فناوری اطلاعات توسط گروهی افراد حرفه‌ای تعلیم‌دیده ۲ الی ۳ ماه به طول می‌انجامد. برطرف کردن مهم‌ترین نقاط ضعف به‌وسیله ایجاد یک شبکه انعطاف‌پذیر با دفاع چند لایه ممکن است چندین ماه به طول انجامد. سپس فرآیند باید به‌طور منظم تکرار شود.

آسیب‌پذیری‌های جدید محتاج رسیدگی مستمر هستند.

فرآیند ایمن‌سازی شبکه‌های اینترنتی و سیستم‌ها باید مستمر باشد، زیرا آسیب‌پذیری‌های جدید پیوسته ایجاد شده یا کشف می‌شوند. CERT/CC خاطرنشان می‌کند که نه تنها موارد و تعداد حملات اینترنتی[1] با نرخ نگران‌کننده‌ای رو به افزایش است، بلکه آسیب‌پذیری‌هایی هم که مهاجم می‌تواند از آنها استفاده کند پیوسته افزایش می‌یابد. آسیب‌پذیری‌های امنیتی کامپیوتری شناخته شده (مشکلات مربوط به نرم‌افزار یا سخت‌افزار که اجازه ورود غیرمجاز یا صدمه زدن به شبکه را می‌دهند) در سال گذشته به بیش از دو برابر رسیده‌اند، یعنی ۱۰۹۰ نقطه ضعف مجزا در سال ۲۰۰۰ گزارش شده که در سال ۲۰۰۱ به ۲۴۳۷ نقطه ضعف رسیده است. نصب و راه‌اندازی یک ابزار امنیت شبکه‌ای نمی‌تواند جایگزین تلاش مستمر برای به‌هنگام‌سازی سیستم‌های دفاعی گردد.

---

1. Internet Attacks

در یک نظرسنجی که اخیراً توسط «مؤسسه امنیت کامپیوتری» انجام شده، ۹۰ درصد پاسخ‌دهندگان از نرم‌افزار ضدویروس استفاده می‌کردند، اما ۸۵ درصد آنان از ویروس صدمه دیده بودند. در همین نظرسنجی، ۸۹ درصد دیوارهای آتشین[1] کامپیوتری نصب کرده بودند و ۶۰ درصد مجهز به سیستم‌های ردیابی و جست‌وجوی مزاحم بودند، اما با این وجود ۹۰ درصد آنان پیشامد رخنه‌های امنیتی[2] را گزارش دادند و به ۴۰ درصد آنان از خارج شبکه نفوذ شده بود.

اکثریت نقاط ضعف امنیتی را می‌توان به‌وسیله روش‌های امنیتی مناسب تقلیل داد. چنانکه آمارهای نظرسنجی بیان می‌کنند، روش‌های مناسب امنیتی فقط شامل نصب ابزارهای یادشده نیست، بلکه استفادهٔ صحیح و به‌هنگام نگاه‌داشتن آنها از جمله، وصله کردن[3] برنامه و به‌هنگام‌سازی ضدویروس‌ها از اهمیت بسزایی برخوردار است.

امنیت اینترنتی و هزینه فرصت

برای شرکت‌ها به‌طور خاص و برای اقتصاد ملی به‌طور اعم، ارتقای امنیت کامپیوتری غالباً محتاج سرمایه‌گذاری زمان، توجه و پول است. رئیس‌جمهور بوش از کنگره درخواست کرد تا سرمایه‌گذاری بر روی ایمن‌سازی کامپیوترهای دولت را در سال مالی ۲۰۰۳ به میزان ۶۴ درصد افزایش دهد.

سرمایه‌گذاری رئیس‌جمهور بوش بر روی ایمن‌سازی شبکه‌های کامپیوتری دولت در نهایت به‌واسطه ارائه ابزارهای کامپیوتری دولت الکترونیک، مدیریت نوین شرکت‌ها و کاهش ضایعات، تقلب و کلاهبرداری موجب کاهش هزینه‌ها خواهد شد.

فقدان سیستم‌های اطلاعاتی ایمن و قابل اطمینان مانعی برای رشد آینده اقتصاد ملی و خصوصاً صنعت فناوری اطلاعات محسوب می‌شود. بخش عمده‌ای از امیدها و پتانسیل‌های

---

1. Firewall
2. Security Bags
3. Patching

ادامه رشد اقتصاد که معلول انقلاب فناوری اطلاعات می‌باشند، هنوز تحقق نیافته است. تحقق نیافتن فرصت‌هایی از قبیل تجارت الکترونیک و فعالیت‌های (B2b معاملات شرکت با شرکت)، تا اندازه‌ای معلول خطرات امنیتی کامپیوتر است. فقدان امنیت اینترنتی تنها معاملات تجاری را به خطر نمی‌اندازد، بلکه دارایی‌های فکری، عملیات تجاری، خدمات زیرساختی و اعتماد جامعهٔ مصرف کنندگان را هم در معرض خطر قرار می‌دهد.

سرمایه‌گذاری بر روی امنیت اینترنتی به معنی هزینه بالاسری اضافی نیست و سود این سرمایه‌گذاری به ما بازمی‌گردد. نظرسنجی‌ها مکرراً نشان داده‌اند که؛

- هزینه‌های ناشی از یک حمله مخرب کامپیوتری به احتمال قوی از سرمایه‌گذاری پیشگیرانه در برنامه امنیت اینترنتی سنگین‌تر هستند.
- طراحی ساختار امنیتی قدرتمند در معماری سیستم‌های اطلاعاتی شرکت می‌تواند هزینه‌های عمومی عملیات را کاهش دهد. این رویه‌های کاهش هزینه در شبکه‌هایی که فاقد امنیت مناسب هستند، امکان‌پذیر نمی‌باشد.
- این نتایج نشان می‌دهد که با بالا بردن سطح آگاهی بیشتر در مورد این موضوعات، شرکت‌ها ممکن است دریابند که افزایش سطح امنیت اینترنتی امکان کسب منفعت بیشتر را برایشان فراهم می‌کند. ارتقای سطح آگاهی و تلاش‌های داوطلبانه، اجزای حیاتی این استراتژی هستند.

مدیریت ریسک در سطح ملی و فردی

پیش از حوادث ۱۱ سپتامبر، خسارات ناشی از شبکه‌های تروریستی خارجی در ایالات‌متحده بسیار محدود بود، اما این روند در عرض یک روز متحول گشت. برآوردهای انجام‌شده میزان افزایش هزینه‌های وارده از حملات تروریستی به سیستم‌های اطلاعاتی ایالات‌متحده را در بخش اقتصاد حدود ۴ برابر در چهار سال گذشته اعلام کرد. هر چند این خسارات نسبتاً محدود است، اما امکان دارد این وضعیت به‌طور ناگهانی تغییر یابد.

هر روز در آمریکا یک شرکت یا کاربر خانگی کامپیوتر در اثر حملات اینترنتی دچار خسارت شده و متضرر می‌شود. میزان این خسارات در سطح شخصی بسیار چشمگیر و حتی شاید فاجعه‌آمیز است. شرایط وقوع چنین حوادثی در سطح ملی برای شبکه‌ها و سیستم‌هایی که کشور به آنها وابسته است، فراهم می‌باشد و این شرایط عبارتند از:

ـ دشمنان بالقوه چنین قصدی دارند.

ـ ابزارهای تخریب در سطحی وسیع در دسترس هستند.

ـ نقاط ضعف سیستم‌های کشور، فراوان و شناخته‌شده هستند.

عوامل بالا بدین معنا است که هیچ استراتژی نمی‌تواند به‌طور کامل خطر را رفع کند، اما کشور می‌تواند و باید برای مدیریت ریسک وارد عمل شده و صدمات بالقوه سوءاستفاده از نقاط آسیب‌پذیر را به حداقل خود برساند. با بیان این مطلب در یک سند عمومی، ما به دشمنان بالقوه خود چیزی اعلام نمی‌کنیم که خود و یا دیگران قبلاً از آن بی‌خبر بوده باشند.

در ۱۹۹۷ یک کمیسیون ریاست‌جمهوری در گزارش عمومی خود خطرات موجود را بیان داشت. در سال ۲۰۰۰ اولین برنامه ملی برای رسیدگی به این مشکل منتشر شد. در سال ۲۰۰۱، رئیس‌جمهور بوش با استناد به این خطرات، فرمان اجرایی خود را مبنی بر اولویت دادن به مسئله اینترنتی و افزایش بودجه حفاظت از شبکه‌های دولتی را صادر کرد. در سال ۲۰۰۲، رئیس‌جمهور نسبت به تحکیم و تقویت امنیت اینترنتی دستگاه‌های دولتی اقدام کرد.

دولت به تنهایی قادر به ایمن‌سازی فضای اینترنتی نخواهد بود.

به‌رغم این هوشیاری‌ها و تدابیر، هنوز هم خطر متوجه شبکه‌های اطلاعاتی ملی ما و سیستم‌های حیاتی تحت اداره آنهاست. کاهش این خطر، مستلزم همکاری فعال و بی‌سابقه میان بخش‌های گوناگون کشور ما و متحدان جهانی آن است.

دولت فدرال نباید و در واقع نمی‌تواند امنیت شبکه‌های کامپیوتری بانک‌های خصوصی، شرکت‌های بخش انرژی، مؤسسات حمل‌ونقل و سایر قسمت‌های بخش خصوصی را تأمین

نماید. دولت فدرال نباید وارد خانه‌ها و کسب و کارهای کوچک، دانشگاه یا ادارات و سازمان‌های محلی شود تا امنیت شبکه‌های کامپیوتری آنها را تأمین کند.

هر آمریکایی که به اینترنت، یعنی مادر شبکه‌های اطلاعات وابسته است باید امنیت بخش مربوط به خود را تأمین کند. دولت فدرال می‌تواند به وسیله تدابیر زیر به ایجاد این توانایی‌ها در ملت آمریکا کمک کند:

- افزایش سطح آگاهی و هوشیاری؛
- در اختیار قرار دادن اطلاعات مربوط به نقاط آسیب‌پذیر و راه‌حل آنها؛
- ترویج شراکت و همکاری دولت با بخش خصوصی، گروه‌های بخش خصوصی با یکدیگر و سایرین؛
- ترغیب به ارتقای فناوری در سازمان‌ها؛
- افزایش تعداد افراد ماهر و آموزش‌دیده؛
- انجام تحقیقات و پیگیری جنایات اینترنتی؛
- حفاظت از کامپیوترهای دولتی؛

ارتقای امنیت شبکه‌هایی که اقتصاد و امنیت ملی به آنها وابسته هستند.

در نهایت، امنیت اینترنتی به معنای «حمله صفرها و یک‌های خوب به صفرها و یک‌های بد در فضای دنیای اینترنت نیست». بلکه بدین معنا است که آیا با قطعی برق توسط تروریست‌ها مواجه می‌شویم، پولی که ملت آمریکا، سرمایه‌گذاری و یا پس‌انداز کرده امنیت خواهد داشت و یا این کشور امنیت دارد یا خیر.

از قرن نوزدهم از زیرساختارهای فیزیکی ایالات‌متحده یعنی زمان ساخته شدن آنها حفاظت شده است. برای مثال، پلیس راه‌آهن به‌منظور کاهش تهدیدات وارد به شبکه‌های عظیم حمل‌ونقل ایجاد شد. مشکلات امنیت فیزیکی هنوز باقی هستند، اما اکنون مشکلات امنیت اینترنتی هم به آن اضافه شده است. این دو گروه مشکلات به یکدیگر مربوطند. یک مشکل

منیت اینترنتی می‌تواند ساختارهای فیزیکی را ناامن کند و بالعکس. دولت و صنعت باید به تحلیل این تعاملات و وابستگی‌های متقابل بپردازند، اما در عین حال باید تلاش‌های خود را به‌طور خاص بر نقاط آسیب‌پذیر جدید و منحصر به فرد ناشی از اتکا به اینترنت متمرکز کنند.

رهنمودها و سیاست‌های ملی

«استراتژی ملی امنیت اینترنتی» مکمل «استراتژی ملی امنیت داخلی» و «استراتژی امنیت ملی ایالات‌متحده» است. بخش «اصول و سیاست‌ها» به همراه فرمان اجرایی رئیس‌جمهور بوش ۱۳۲۳۱ رهنمودهای سیاست دولت راجع به امنیت اینترنتی را بیان می‌دارد. بیانیه‌های سیاست و توصیه‌های ارائه‌شده در این سند استراتژی مشروط به فرمان اجرایی ۱۳۲۳۱ و سایر فرمان‌های اجرایی مربوطه، راجع به امنیت ملی هستند و در اینجا هیچ‌یک از اختیارات، نقش‌ها و مسئولیت‌های ایالات‌متحده تحت «قانون امنیت ملی» یا سایر قوانین مربوطه را تغییر نمی‌دهد.

این سند، تاکنون اولین «استراتژی ملی امنیت اینترنتی» به‌شمار می‌رود. هدف این استراتژی، مشارکت، ایجاد توانمندی‌ها و هماهنگ کردن تلاش‌ها جهت تأمین امنیت اینترنت است. مشارکت دادن و ایجاد توانمندی در ملت آمریکا برای تأمین امنیت اینترنت، مأموریتی پیچیده است که محتاج تلاش‌های هماهنگ و متمرکز جامعه اعم از دولت فدرال، ایالات و دولت‌های محلی، بخش خصوصی و مردم آمریکا است. هدف از این استراتژی، اجرای اصول و اهداف سیاست‌های ملی رئیس‌جمهور جهت تأمین امنیت اینترنتی است.

بیانیه سیاست ملی

انقلاب فناوری اطلاعات، روش‌های انجام معاملات تجاری، عملیات اجرایی دولت و دفاع ملی را متحول ساخته است. این سه کارکرد اکنون به یک شبکه به هم وابسته از زیرساختارهای حیاتی اطلاعات ـ اینترنت ـ وابسته هستند.

به‌منظور به حداقل رساندن اختلالات و ارتقای قابلیت اطمینان، محتاج تلاش‌های مستمر جهت ایمن‌سازی سیستم‌های اطلاعاتی زیرساختار حیاتی، از جمله؛ ارتباطات، بسیج اضطراری و همچنین امکانات فیزیکی برای پشتیبانی این سیستم‌ها هستیم.

ایالات‌متحده به توانایی حفاظت زیرساختارهای حیاتی کشور در برابر حوادث طبیعی و حملات هدفمند دست خواهد یافت. این تهدیدات شامل مواردی هستند که به توانایی‌های ذیل، لطمات جدی وارد می‌سازند؛

- توانایی.دولت فدرال به‌منظور اجرای مأموریت‌های حساس امنیت ملی، امنیت داخلی و تضمین سلامت و امنیت عمومی جامعه.

- توانایی دولت‌های ایالتی و محلی به‌منظور حفظ نظم و ارائه خدمات زیرساختاری عمومی و ضروری.

- توانایی بخش خصوصی به‌منظور کارکرد منظم اقتصاد و ارائه خدمات زیرساختاری ضروری.

این سیاست خاطرنشان می‌سازد که تدابیر امنیتی هیچ‌گاه قابلیت اطمینان صد درصد را ندارند. اما، با این وجود سعی می‌شود هرگونه اختلال یا تخریب کارکردهای زیرساختی،نادر، کوتاه‌مدت، قابل رفع و از نظر جغرافیایی ایزوله (منفرد) باشد و لطمات وارده به رفاه ایالات‌متحده به حداقل ممکن رسانده شود.

بسیاری از زیرساختارهای اساسی کشور به‌طور سنتی، سیستم‌هایی مجزا و مستقل از یکدیگر و از لحاظ فیزیکی و منطقی با همبستگی بسیار اندک بوده‌اند. ولی پیشرفت‌های فناوری اطلاعات و لزوم بهبود کارایی، میزان اتوماسیون و ارتباط متقابل بین این سیستم‌ها را به‌طور فزاینده و مستمری افزایش داده است.

«لایحه میهن‌پرستی آمریکا» زیرساختار حیاتی را بدین‌گونه تعریف می‌کند؛ «سیستم‌ها و دارایی‌های حیاتی برای ایالات‌متحده، اعم از فیزیکی یا مجازی که تضعیف یا نابودی آنها اثر مخرب و جدی بر امنیت کشور، امنیت اقتصاد ملی، ایمنی یا بهداشت عمومی کشور و یا

ترکیبی از این موارد خواهد گذاشت». زیرساخت‌های حیاتی آمریکا شامل انرژی (برق، نفت و گاز)، حمل‌ونقل (راه‌آهن، خطوط هوایی و تجارت دریایی)، امور مالی و بانکداری، اطلاعات و مخابرات، بهداشت عمومی، خدمات اضطراری، آب، موادشیمیایی، دولت، صنایع دفاعی، صنایع غذایی، کشاورزی و پستی و حمل‌ونقل کالاها است.

همچنین استراتژی تصدیق می‌کند که حفظ تمامیت اقتصادی و اجتماعی ملی در بلندمدت، نه تنها مستلزم توجه به امنیت سیستم‌های اطلاعاتی است، بلکه باید به ساختارهای اجتماعی مربوطه که این سیستم‌ها به آنها وابسته‌اند، هم توجه شود. بالطبع، استراتژی حاضر تدابیری برای تقویت و تحکیم این ساختارهای پشتیبانی اندیشیده است.

هر چند ایالات‌متحده آمریکا دارای قوی‌ترین نیروی نظامی و بزرگ‌ترین اقتصاد ملی در سطح جهان است، اما این دو نماد قدرت ملی به‌طور فزاینده‌ای به زیرساخت‌های حیاتی خاص، از جمله سیستم‌های اطلاعاتی اینترنتی وابسته هستند. همان‌طور که در ۱۱ سپتامبر شاهد بودیم، دشمنان آمریکا، اعم از دولت‌ها، گروه‌ها و حتی اشخاص، برای انجام حملات غیرمتعارف آمادگی کسب کردند. این دشمنان به‌طور صریح قصد خود مبنی بر حمله به شهروندان آمریکا و همچنین قلمرو اینترنتی و زیرساخت‌های ملی یعنی ارکان اقتصاد ما را اعلام کرده‌اند.

رهنمودهای سیاست‌ها

در ژانویه ۲۰۰۱، دولت مطالعات خود درباره نقش سیستم‌های اطلاعاتی و امنیت اینترنتی را آغاز کرد و در اکتبر ۲۰۰۱، رئیس‌جمهور بوش دستور اجرایی ۱۳۲۳۱ را صادر نمود. این دستور، مشتمل بر آغاز برنامه حفاظتی تأمین امنیت سیستم‌های اطلاعاتی زیرساخت‌های حیاتی، از جمله ارتباطات، شرایط اضطراری و دارایی‌های فیزیکی پشتیبانی‌کننده این سیستم‌ها بود. حفاظت از این سیستم‌های اینترنتی برای تمامی بخش‌های مختلف اقتصاد ضروری است.

تهیه و اجرای دستورات این برنامه با رعایت اصول سازمان‌دهنده زیر صورت گرفته است:

مشارکت‌های خصوصی ـ دولتی

حفاظت از زیرساخت‌های حیاتی لزوماً یک مسئولیت مشترک است، زیرا تقریباً ۸۵ درصد تسهیلات زیرساخت‌های حیاتی کشور تحت مالکیت و مدیریت بخش خصوصی است و بسیاری از عملیات‌های حیاتی دولت نیز وابسته به این تسهیلات خصوصی می‌باشد.

از آنجا که تسهیلات دولت و بخش اقتصاد، هر دو هدف حملات دشمنان به زیرساخت‌های حیاتی ملی است، رسیدگی به نقطه ضعف‌های بالقوه، نیاز به رویکردهای انعطاف‌پذیر و تکاملی دارد که هر دو بخش خصوصی و دولتی را تحت پوشش قرار دهد و از هر دو جنبه داخلی و بین‌المللی، امنیت منابع کشور را تأمین نماید. بخش خصوصی با تلاشی بسیار هماهنگ و جدی برای رسیدگی به این مشکلات با دولت فدرال همکاری کرده است. یکی از گام‌های مهم بسیاری از بخش‌ها، ایجاد «مراکز تجزیه و تحلیل و تبادل اطلاعات» (ISAC) به‌منظور تسهیل ارتباطات و انتشار اطلاعات امنیتی است. افزون بر این، بخش‌های مختلف طرح‌هایی برای ایجاد امنیت در بخش اینترنتی خود تهیه کرده‌اند که مکمل این استراتژی ملی می‌باشد. عزم دولت نیز بر آن است تا این مشارکت و همکاری مؤثر و مفید همچنان ادامه یابد.

کشور باید تلاش‌های خود را بر روی مکانیزم‌های پیشگیری و مدیریت بحران مشتمل بر شناسایی و مرتفع ساختن نقاط آسیب‌پذیر، آموزش، تحقیق و توسعه، متدولوژی‌های اعلان خطر و تدارک تدابیری برای حمایت از این تلاش‌ها متمرکز کند. بدین منظور، مالکان و متصدیان بخش خصوصی باید تشویق شوند تا حداکثر امنیت ممکن را برای زیرساخت‌های تحت کنترل خود تأمین نمایند و اطلاعات لازم جهت یاری دولت در انجام این وظیفه را در اختیارش قرار دهند. دولت فدرال به سهم خود باید در حراست از سیستم‌های اطلاعاتی خویش، برای بخش خصوصی در زمینه چگونگی تضمین امنیت زیرساخت‌ها، الگو و نمونه باشد و تا بیشترین حد ممکن، نتایج تلاش‌های خود را در اختیار بخش خصوصی گذارد.

اجتناب از وضع مقررات

دولت فدرال چنین تشخیص داده است که به‌منظور جلب همکاری همه‌جانبه بخش خصوصی، مشارکت مالکان و متصدیان بخش خصوصی در شراکت خصوصی ـ دولتی باید به‌صورت داوطلبانه صورت گیرد. دولت آمریکا برای تشویق بخش خصوصی به مشارکت هر چه بیشتر، تا حد ممکن به‌دنبال راه‌هایی است که از تحمیل مقررات دولتی یا تکلفات اضافی از سوی دولت بر بخش خصوصی بدون تأمین پشتوانه مالی اجتناب نماید. بنابراین دولت در رسیدگی به مشکلات حفاظت از زیرساخت‌های حیاتی به‌عنوان گزینه اول خود متکی بر پاداش‌های بازاری بوده و تنها در صورتی‌که بازار به‌طور محسوس در حفاظت از بهداشت، ایمنی یا رفاه مردم آمریکا ناموفق عمل کند به وضع مقررات اضافی روی خواهد آورد.

حراست از آزادی‌های مدنی و حریم شخصی

منافع امنیتی و حریم شخصی لزوماً تضادی با یکدیگر ندارند. در واقع تدابیر اتخاذشده در این استراتژی با تضمین امنیت و سلامت ارتباطات اینترنتی به‌دنبال حفاظت از حریم شخصی افراد بوده و بنابراین مکمل این منافع، حریم شخصی می‌باشند. با این حال، در اتخاذ تدابیر جهت ارتقای امنیت کشور باید دقت لازم لحاظ گردد تا ارزش‌های بنیادین و ویژگی‌های جامعه آزاد که کشور در درجه اول به‌دنبال حفاظت از آنهاست، تضعیف نگردد. بنابراین باید دقت شود تا حریم شخصی و سایر آزادی‌های مدنی محترم شمرده شود. مصرف‌کنندگان و متصدیان باید اطمینان داشته باشند که اطلاعات طوری دقیق، محرمانه و قابل اطمینان به‌کار گرفته می‌شوند.

هماهنگی با کنگره

برای تضمین اینکه رویکردهای اتخاذشده جهت تأمین امنیت سیستم‌های اینترنتی آمریکا از اتفاق‌نظر و حمایت گسترده‌ای برخوردارند، قوه مجریه درباره رویکردها و برنامه‌های خود با

کنگره همکاری خواهد نمود تا اهداف سیاست ملی را برآورده نماید. در صورت مقتضی، قوه مجریه می‌تواند از کنگره درخواست کند تا قوانینی برای پیشبرد این استراتژی به تصویب رساند.

همکاری با دولت‌های محلی و ایالتی

دموکراسی آمریکا، ریشه در اصول فدرالیسم دارد، یعنی سیستم حکومتی که در آن دولت‌های ایالتی در حکومت با دستگاه‌های فدرال (مرکزی) سهیم‌اند. این ساختار هم پوشاننده دولت فدرال، ایالتی و محلی بیش از ۸۷۰۰۰ حوزه قضایی دارد و فرصت‌ها و چالش‌های منحصر به فردی در نیل به امنیت اینترنتی پدید می‌آورد. دولت‌های ایالتی و محلی همانند دولت فدرال، سیستم‌های اطلاعاتی بزرگ و به هم مرتبطی دارند که خدمات حیاتی دولت، به آنها وابسته است.

فرصت موجود، از تخصص و تعهد دستگاه‌ها و سازمان‌های محلی متصدی امنیت اینترنتی نشأت می‌گیرد و چالش موجود، ایجاد سیستم‌های به هم مرتبط و مکملی است که کار یکدیگر را تقویت نمایند، نه اینکه دوباره‌کاری کنند و همچنین اطمینان حاصل شود که نیازمندی‌های ضروری مورد انتظار از سیستم برآورده می‌گردد. بنابراین، کلیه اقدامات و برنامه‌های حفاظت زیرساخت‌های حیاتی و فضایی اینترنت باید نیازها، فعالیت‌ها و مسئولیت‌های دولت‌های محلی و ایالتی و کاربران نهایی را مدنظر قرار دهند.

تعیین دستگاه‌های هماهنگ‌کننده

دولت، برای تسهیل و تقویت هماهنگی و ارتباط دولت فدرال و بخش خصوصی که شراکت مؤثر بین آنها بدان وابسته است، یک دستگاه مسئول برای هر یک از بخش‌های اصلی اقتصاد که در برابر حملات زیرساختی آسیب‌پذیرند، تعیین کرده است. به علاوه، «اداره سیاستگذاری علوم و فناوری» (OSTP) تحقیقات و توسعه در زمینه پشتیبانی از حفاظت

زیرساخت‌های حیاتی را هماهنگ می‌کند. (اداره مدیریت و بودجه (OMB)) «معادل با سازمان مدیریت و برنامه» مسئول تدوین، تصویب و نظارت اجرایی بر سیاست‌ها، اصول، استانداردها و رهنمودهای موردنظر برای برنامه‌های امنیت کامپیوتری دولت فدرال است. وزارت امورخارجه مسئول هماهنگی امور امنیت اینترنتی در حوزه بین‌المللی محسوب می‌شود. رئیس اداره اطلاعات مرکزی (CIA)، مسئول ارزیابی تهدیدات خارجی است که متوجه سیستم‌های اطلاعاتی و شبکه‌های ایالات‌متحده می‌باشد. قوه قضائیه و اداره بازرسی فدرال (FBI) تلاش‌های ملی در انجام تحقیقات و پیگرد قانونی جرائم اینترنتی را هدایت می‌نمایند.

نمایندگان بخش‌ها و دستگاه‌های مسئول با همکاری یکدیگر، نقاط آسیب‌پذیر بخش خود را در مقابل حملات فیزیکی و اینترنتی ارزیابی کرده و طرح‌ها یا تدابیری برای حذف نقاط آسیب‌پذیر پیشنهاد می‌دهند. از آنجا که فناوری و ماهیت تهدیداتی که زیرساخت‌های حیاتی ملی با آن مواجه هستند به سرعت و به‌طور مداوم تغییر می‌کنند، بخش‌ها و دستگاه‌های مسئول باید به‌طور مرتب قابلیت اطمینان، نقاط ضعف و بسترهای تهدیدکنندهٔ زیرساخت‌های ملی را ارزیابی کرده و اقدامات و واکنش‌های حفاظتی را در پیش بگیرند که توانمند و سازگار باشد. سرانجام، در عین حفظ رابطه شراکتی باید از اختیارات، توانایی‌ها و منابع دولت از جمله انتظام و پیاده‌سازی قوانین، وضع مقررات، جاسوسی خارجی و آمادگی دفاعی به‌طور کامل و به‌صورت مقتضی برای تحقق حفاظت زیرساخت‌های حیاتی و تداوم آن بهره‌برداری شود.

اصول راهبردی

استراتژی ملی امنیت اینترنتی ثمرهٔ تلاش‌های افراد، گروه‌ها و مؤسسات در اقصی نقاط کشور است. هدف نهایی این تلاش‌ها، ایجاد یک زیرساخت ایمن، مورد اعتماد، توانمند، قابل اطمینان و استفاده، به‌منظور پشتیبانی اقتصاد، امنیت ملی و خدمات حیاتی آمریکا در آینده نزدیک می‌باشد.

دنیای مجازی اینترنت، شبکه‌ای پیچیده است که زیرساخت‌ها، شرکت‌ها و ملل مختلف را

به یکدیگر متصل می‌کند. این اتصالات بر روی مسیرهای متعددی صورت می‌گیرد که تحت تملک گردانندگان مختلف است. تأمین امنیت این شبکه به معنای اینکه هیچ عضو یا مسیر ارتباطی از این شبکه قطع نمی‌شود، نیست. بلکه بدین معناست تا اطمینان حاصل شود که:

۱. شبکه در مقابل اختلالات یا نابودی مسیرها انعطاف‌پذیر است

۲. مسیرها را می‌توان با یکدیگر جایگزین کرد

۳. اجزای اضافی (جهت اطمینان) در شبکه فراوانند

۴. از کار‌انداختن دائمی آنها مشکل است. امنیت اجزای منفرد در فضای اینترنت و تکامل مستمر آنها با تغییر شرایط، این انعطاف‌پذیری را ایجاد می‌نماید.

بنابراین برای ایجاد یک شبکه اینترنتی امن و انعطاف‌پذیر، کشور باید دو اصل راهبردی امنیت را پذیرفته و اجرا کند؛

الف) امنیت کل زیرساخت به امنیت هر یک از اجزا بستگی دارد.

ب) تهدیدات و نقاط آسیب‌پذیر پیشرفت می‌کنند و امنیت هم طبعاً باید همگام با آنها یا سریع‌تر از آنها پیشرفت کند.

تأمین امنیت در اجزای دنیای اینترنت منجر به تأمین امنیت کل مجموعه خواهد شد.

امنیت اینترنت به امنیت تمام اجزای آن وابستگی دارد. در دنیای اینترنت، مهاجمان می‌توانند با سرعت نور به هر مکانی برسند، هیچ‌گونه ایمنی جغرافیایی وجود ندارد، شبکه‌ها ممکن است هم در مقابل حملات از داخل شبکه و هم در مقابل حملات از خارج از آن آسیب‌پذیر باشند. اجزای شبکه که به‌نظر ایمن هستند، ممکن است توسط کارکنان داخلی (خودی‌ها)، نرم‌افزارهای دانلود شده (پیاده شده) و یا شبکه‌های آلوده همسایه مورد تهاجم قرار گیرند. کشیدن دیوار دور شبکه، برای رسیدن به امنیت کافی نیست. به محض اینکه یک کامپیوتر یا جزئی از شبکه مورد تهاجم قرار گرفت، آن جز می‌تواند برای تهاجم به سایر اجزا مورد استفاده قرار گیرد.

به‌طور مشابه، بخش‌های فاقد امنیت اقتصاد یا دولت می‌توانند به‌عنوان سکوهای حمله به سایر بخش‌های زیرساختار استفاده شوند و می‌شوند.

همچنین، اختلال در یک بخش اثرات تصاعدی دارد که می‌تواند به اختلال سایر اجزای زیرساخت هم بینجامد. به‌منظور مبارزه با این نقاط آسیب‌پذیر، سیستم‌ها باید طوری طراحی شوند که امنیت زیرساخت به یک لایه یا گروه واحد و یا نقطه مرکزی وابسته نباشد، بلکه باید در چندین لایه شکل بگیرد، سیستم‌های دفاعی، توزیعی (پراکنده) باشد و توانایی ترمیم سریع پس از هر حمله را داشته باشد. برای بهبود امنیت اینترنتی، کشور باید در تمامی سطوح فعالیت در دنیای اینترنت، امنیت لازم را فراهم نماید. بنابراین هر فرد و بخشی باید از نقش و مسئولیت‌های خود در ایجاد امنیت در حوزه فعالیت خویش آگاه باشد. هر بخش و هر فرد برای ایجاد امنیت در دنیای اینترنت به سایرین وابسته است. بنابراین کشور باید از طریق آگاهی‌دهی و اطلاع‌رسانی، شناساندن نقش‌ها و مشارکت‌ها در کلیه سطوح و تأمین امنیت سیستم‌های اینترنتی دولتی تحت رهبری خود دولت فدرال به تأمین امنیت اینترنتی بپردازد. چنین رهبری همچنین شامل جلوگیری و ممانعت از جرائم اینترنتی، جاسوسی الکترونیک و جنگ اطلاعاتی هم خواهد بود.

بهنگام سازی و تکامل سریع تدابیر امنیتی به‌منظور پیش‌دستی بر فناوری‌ها و نقاط ضعف جدید

نقاط ضعف جدید در سیستم‌ها با سرعت نگران‌کننده‌ای در حال افزایش‌اند. این نقاط ضعف، با نوشته شدن نرم‌افزارهای جدید و پیدایش فناوری‌های جدید به‌وجود می‌آیند. آنها با گذشت زمان و به‌کارگیری نرم‌افزارها مشخص می‌شوند. این در حالی است که ابزارهای جدید و بسیار پیشرفته‌تری برای بهره‌برداری از این نقاط ضعف ساخته می‌شوند.

سیاست‌ها، رویه‌ها و فناوری‌های امنیتی هم باید خود را همگام با آنها به‌هنگام سازند. کشور باید زیرساخت امنیتی ایجاد نماید که بتواند همواره یک گام جلوتر از مهاجمان

احتمالی باشد. متخصصان به تازگی دریافته‌اند، نانوتکنولوژی[1] و امکانات محاسبات (کامپیوتری) کوانتومی چه اثری می‌تواند بر دنیای اینترنت فعلی بگذارد. نوآوری‌های یادشده و سایر نوآوری‌ها، تغییرات شگرف و غیرقابل پیش‌بینی در نحوه عملکرد شبکه‌ها و نحوه تأمین امنیت آنها به‌وجود خواهد آورد.

کشور ما برای آنکه این تغییرات را درک کند و همچنان رهبر جهان در توسعه و کاربرد فناوری‌های جدید در امنیت اینترنتی باقی بماند، باید در زمینه‌های آموزش و پرورش، فناوری و هماهنگی فعالیت‌ها سرمایه‌گذاری کند.

ـ کلاهبرداری اینترنتی از ۱۰۰ هزار نفر

برای ماتیو بووین که اکنون به جرم کلاهبرداری در زندان سانتا کروز به سر می‌برد، استفاده از اینترنت مفهوم دیگری داشت. وی توانست توسط اینترنت، ۱۰۰,۰۰۰ نفر را طعمه خود نموده و سرمایه‌هایشان را برباید!! روش کاری او اعلان آگاهی در سایت پرتردد سرمایه‌گذاری بود که با حیله‌ای آنان را وادار به سرمایه‌گذاری در شرکت‌های بی‌ارزش می‌کرد. این عمل تنها توسط وب و با استفاده از تکنولوژی بالای[2] آن انجام می‌گرفت.

اساس کار بووین به این صورت بود که در آگهی‌ای که در قسمت Products & Services داده بود مدعی شد که شرکتی به نام Netcaller & Pcremote می‌تواند انقلابی عظیم در بخش‌های مختلف اینترنت ایجاد کند و از این شرکت به‌عنوان تازه‌ترین شریک مایکروسافت یاد می‌کرد. در اصل کلیه این اطلاعات دروغ بود و هرگز مشارکتی با مایکروسافت وجود نداشت و مهندسان و مشاورانی که تحت نام «نفرات کلیدی شرکت» Netcaller & Pcremote عنوان می‌شدند، عملاً هیچ ارتباطی با این شرکت نداشتند. به‌خاطر اولین آگاهی، حدود ۳۰۰۰ نفر از اقصی نقاط دنیا از طریق پیک الکترونیک[3] از بووین اطلاعات خواستند و حتی ۱۵۰ نفر

1. Nanotechnology
2. High Technology
3. E-mail

از این جمع، چک‌های سرمایه‌گذاری خود را فرستادند که در بین این افراد می‌توان به دو مورد اشاره کرد که مورد اول از هنگ‌کنگ با سرمایه‌گذاری حدود ۱۰۰۰۰ دلار و مورد دوم از کالیفرنیا با مبلغی حدود ۱۵۰۰ دلار بود. طی سه ماه بووین توانست ۱۹۰۰۰۰ دلار پول از این طریق به‌دست آورد!! خوشبختانه بووین، کلاهبردار خوبی نبود و در آوریل ۱۹۹۸ دستگیر و زندانی شد، اما خسارت سرمایه‌گذاری در این قبیل موارد را چه کسی می‌پردازد؟

در این‌باره استیون فوجیتا که یکی از قربانیان بووین است، می‌گوید: «حدس می‌زنم باید مراقب شرکای بعدی مایکروسافت باشم». او هزار دلار در بازی بووین از دست داده است. در حال حاضر با این نحوه کلاهبرداری، میلیون‌ها نفر قربانی و شکار می‌شوند و این در حالی است که تا چند سال پیش چنین پدیده‌ای وجود نداشت. سازمان امنیت معاملات و مبادلات حق‌العمل کاری (Securities and Exchange) یا Sec در سال ۱۹۹۶ تأسیس شد که اساس فعالیت آن نظارت بر نحوه معاملات بود. در آن زمان، این سازمان در هر روز بیش از ۱۰۰ مورد شکایت در مورد شرکت‌های دروغین داشت که این رقم در حال حاضر به یک مورد در سال رسیده است.

اما به‌نظر می‌رسد که این آمار هنوز ایده‌آل نیست. بزرگ‌ترین عامل شکست و یا عدم موفقیت کامل Sec این است که اکثر سرمایه‌گذاران دوست ندارند که از نحوه و نوع معاملاتشان اطلاعاتی بدهند و در پاره‌ای اوقات برخی از افراد با استفاده از این نحوه تفکر، سرمایه‌گذاران را تشویق به سرمایه‌گذاری پروژه‌های سالی فوری و مخفیانه کرده و بسیاری را از این طریق طعمه خود می‌کنند. با توجه به اینکه در عصر ما لزوم استفاده از اینترنت در امر سرمایه‌گذاری امری بدیهی و عادی است، امروزه تنها با یک تماس ساده توسط شبکه‌ها و سایت‌های مختلف اینترنت می‌توان میلیون‌ها نفر را بدون آنکه انجام این عمل هزینه بالایی داشته باشد، شکار کرد. بنابر آخرین آماری که توسط مؤسسه Jupiter Communication استخراج شده است، تنها در آمریکا حدود ۱۰ میلیون نفر از وب جهت سرمایه‌گذاری‌های گوناگون استفاده می‌کنند.

این آمار اضافه می‌کند در حدود ۳۰۰۰۰۰۰ نفر سیستم معاملاتی مستقیم یا معامله توسط اینترنت را برای پرداخت‌های خود برگزیده‌اند. کارشناسان معتقدند این تعداد در ۳ سال آتی به ۱۴ میلیون نفر می‌رسد Silicon Investor یکی از سایت‌های محبوبی است که در روز حدود دوازده هزار نفر برای گفت‌وگو درباره ارزش سهام به آن سر می‌زنند. Stock Master از دیگر سایت‌های معروف و یکی از مراکز مهم اطلاع‌رسانی در آمریکا است. تعداد تماس‌هایی که با این مرکز گرفته می‌شود به ۷۰۰۰۰۰ مورد در طول روز می‌رسد، در حالیکه این تعداد در سال ۱۹۹۶ تنها به ۵۰۰۰ مورد در روز می‌رسید و طبیعی است که با توجه به حجم بالای فعالیت این مراکز، امکان سوءاستفاده و کلاهبرداری نیز بسیار زیاد است.

در گذشته نه چندان دور مطالعه و تصمیم‌گیری بر روی سرمایه‌گذاری کاری بسیار دشوار بود و طبعاً یک نقشه‌کش ماهر در سوءاستفاده‌های مالی مجبور بود با انجام صدها تلفن در اجرای نقشه‌اش موفق شود، اما امروزه افرادی مانند بووین حتی یک سکه ۱۰ سنتی در جهت اجرای نقشه‌هایشان خرج نمی‌کنند. در سال ۱۹۹۵ اولین پرونده کلاهبرداری که توسط Sec بررسی شد، مربوط به سهام شرکت Pleasure Time بود. روش کار بدین ترتیب بود که آنها افرادی را اجیر کرده بودند تا از طریق اینترنت دیگران را تشویق به خرید سهام این شرکت کنند. در عصر اینترنت، این روش قدیمی و بسیار کودکانه به‌نظر می‌رسید.

روش شرکت System of Excellence یک طرح نخ‌نمای قدیمی است؛ صاحبان این شرکت با دادن رشوه به سردبیر یک خبرنامه اینترنتی از او خواستند تا در مورد سهام شرکت‌های بی‌ارزش مطالب غیرواقعی نوشته و آنها را با ارزش اعلام کنند تا مشتریان با خواندن این اخبار دروغین حاضر به سرمایه‌گذاری در این شرکت‌ها شوند. Elector-Optical از زمره این شرکت‌هایی است که در فاصله‌ای ۳ ماهه توانست با نشر اخبار دروغین، ارزش سهامش را از ۵۰ سنت به ۷ دلار برساند. از طریق این نوع کلاهبرداری ۲ میلیون نفر در اقصی نقاط جهان ۱۰ میلیون دلار از دست دادند. ناشر این روزنامه اینترنتی یک سال به زندان رفت و چارلز هوتو صاحب System of Excellence تنها محکوم به ۲۴ ماه زندان شد. مثال دیگر،

یک شرکت جعلی به نام Octagon Technology بود که با انتشار مجله‌ای به نام اخبار مالی جهان[1] بر روی شبکه اینترنت خود را معرفی کرده و توانست سهام قلابی اکتاگون را به عموم پیشنهاد کند. اساس کار این شرکت به همراه System of Excellence براساس یک طرح و شیوه قدیمی است که در آن طنابی را دست کسی می‌دهی تا داخل چاهی برود و پس آنکه به تو اطمینان کرد، طناب را رها کرده و یا به بیان ساده‌تر اول توسط نشر اخبار غیرواقعی و ترغیب‌کننده در مورد سهام شرکت‌های بی‌ارزش، سرمایه‌گذاران را تشویق به سرمایه‌گذاری کرده و سپس با بالا رفتن تعداد سهام فروخته‌شده ناگهان ناپدید می‌شدند.

این روش اولین بار در سال‌های ۱۷۰۰ توسط کلاهبرداران بازار خرید و فروش لندن استفاده می‌شد که در آن زمان افراد سودجو با بزرگ کردن شانس موفقیت در سرمایه‌گذاری در آمریکای جنوبی به راحتی اداره کل مبارزه با جرائم خاص و رایانه‌ای کلاه را فریب می‌دادند. بعدها در سال ۱۹۸۰ بارها از این روش جهت کلاهبرداری استفاده شد. ولی تفاوت کلاهبرداری از طریق اینترنت در مقایسه با روش‌های پیشین این است که کلاهبرداران منتظر می‌مانند تا قربانیانشان به سمت آنها بیایند، بنابراین نیاز به تعقیب افراد ندارند. گلن اکین یکی از قربانیان بود. او یک مهندس بیکار بود که در ناامیدی بسیار، احتیاج به موقعیتی داشت تا با سرمایه‌گذاری اندک بتواند در مدتی کم به سوددهی بالا برسد.

در ژانویه ۱۹۹۸، هنگامی که او در جست‌وجوی موقعیتی استثنایی در بازار سهام در وب مشغول بود، ناگهان با این خبر که از سوی یک نشریه خبری پخش شده بود، روبرو گشت که وجود بازارهای پرسودی را در آینده‌ای نزدیک خبر می‌داد و با اعلام اینکه با خرید آن می‌توانید در عرض یک سال به بالاترین ارزش افزوده‌ای آن برسید، مواجه شد. اطلاعات اولیه در مورد این سهام متعلق به شرکتی به نام Electro-Optical است که مقر آن در بوستون می‌باشد و با استفاده از تکنولوژی بالای خود سعی در تولید نوعی از سیستم‌های شناسایی اثرانگشت دارد و تخمین می‌زد که در عرض سه ماه سهام این شرکت تا ۳۰۰ درصد افزایش

1. World Financial Report

یابد. اکین با خرید ۴۰۰۰ سهم از قرار هر سهم ۶ دلار، ۲۴۰۰۰ دلار که معادل ۱/۳ از پس‌اندازش بود را در این راه سرمایه‌گذاری کرد. در ابتدا، همه چیز به خوبی پیش می‌رفت و در فاصله ۲ ماه هر سهم به اندازه یک دلار ترقی می‌کرد. اکین در جریان سفرش به بوستون تصمیم گرفت ملاقاتی از این شرکت داشته باشد، اما او این ملاقات را با آنان مطرح نکرد. یک ملاقات غیرمنتظره طبیعتاً نتیجه غیرمنتظره‌ای داشت! در اواسط روز، وقتی او به آدرس موردنظر مراجعه کرد هیچ‌کس را در آنجا ندید و این مسئله به‌نظر عجیب می‌آمد و ... در گزارشی که از سوی Sec ارائه گردیده است، اعلام شد که طی زمستان گذشته شرکت تقلبی نام برده موفق به اختلاس ۱۵ میلیون دلار شده است. تکنولوژی برتر این شرکت هرگز آماده ارائه به بازار نبوده و هرگز قراردادی با هیچ شرکتی منعقد نکرده است.

مقامات قضایی می‌گویند که معاملات بازار سهام آنها عادی نبوده و عامل ایجاد این حجم بالای معاملات به‌صورت مصنوعی، شخصی به نام توماس کاوانا است. خود کاوانا از صحبت کردن با مطبوعات طفره می‌رود، اما وکیل مدافع او ادعا می‌کند که وی نیز قربانی این جریان شده است. نقطه ضعفی که در وب مشاهده می‌شود این است که برای سوءاستفاده‌کنندگان و طراحان نقشه‌های کلاهبرداری همان اندازه امکانات موجود است که برای سرمایه‌گذاران واقعی که قصد فعالیت‌های تجاری سالم را دارند. در این حالت اینترنت، مانند یک شمشیر دو لبه عمل می‌کند. در حال حاضر Sec با استفاده از نرم‌افزار Netwatch سعی در ایجاد محیط امنی برای معامله‌کنندگان واقعی دارد.

طی چهار ماه گذشته تنها در ایالت ایلی نویز، حدود ۳۰۰ مورد مشکوک کشف شد و این در حالی است که نیروی قضایی عملاً نقشی اساسی در پیگرد قضایی این قبیل پرونده‌ها ندارد. دراین‌باره بیل مک دونالد، معاون اجرایی ایالت کالیفرنیا می‌افزاید؛ اگر فردی در کالیفرنیا، شخصی در آمستردام را فریب دهد، عملاً از ما کاری ساخته نیست. اکنون با ایجاد Silican Investor و نرم‌افزارهای مختلف و آدرس http://www.techstock.com می‌توان تا حدودی در برابر کلاهبرداران مالی اینترنت احساس امنیت کرد. ملکه مجموعه این تشکیلات

غیررسمی، خانمی ۵۰ ساله به نام «جنیس شل» می‌باشد. وی یک مورخ هنری و ساکن میلان است.

جنیس شل، در سال پیش یکی از قربانیان سرمایه‌گذاری‌های قلابی در اینترنت شد و در حال حاضر با دقت و وسواس بسیار در جست‌وجوی تبهکاران بر روی شبکه است. وی در این باره خاطره‌ای از جست‌وجوهایش را بیان می‌کند؛ «در ژوئن گذشته، پیغامی از شرکتی به نام Mountion Energy دریافت کردم که بسیار عجیب بود. این شرکت ادعا می‌کرد با سرمایه‌گذاری بر روی سهامش به زودی قادر خواهید بود از سود بالایی برخوردار شوید». با دریافت این پیام، شل تحقیقاتش را آغاز کرد و نتایج به‌دست آمده کاملاً طبیعی به‌نظر می‌رسید، زیرا آن شرکت به جرم کلاهبرداری تحت تعقیب بود و همچنین دارایی‌های این شرکت که عنوان می‌شد، ۲۰۰ میلیون دلار است در واقع رقمی کمتر از صد هزار دلار بود.

در فاصله ژوئن تا آگوست، شل نتیجه تحقیقاتش را به Silican Investor داد و به سرمایه‌گذاران هشدار داد تا از این دام بگریزند. از دیگر تجربیات شل می‌توان به موردی درباره شرکتی به نام FBN اشاره کرد. این شرکت ظاهری قانونی و بسیار موجه برای خود به‌وجود آورده بود که دعای خیر پاپ را دریافت کرده است! اما میزان علاقه مردم به این شرکت افزایش نمی‌یافت، زیرا آگاهی مردم توسط افرادی چون شل و سازمان‌هایی همچون Sec افزایش یافته بود. به زندان سانتا کروز بازمی‌گردیم جایی‌که ماتیو بووین منتظر دادگاه خویش است و دفاع در مقابل اتهاماتش را شخصاً بر عهده گرفته است، اما از این بابت نگرانی خاصی ندارد. بالاترین محکومیتی که می‌توان برای او در نظر گرفت تنها ۸ سال است. او حتی می‌تواند با پرداخت وثیقه آزاد شود. ولی برای ماتیو بووین و دیگر همکارانش مدت زیادی این شانس وجود نخواهد داشت که دارای محکومیت‌های این‌چنینی باشند.

● **چگونه از رایانه خود در برابر ویروس‌های اینترنتی محافظت کنید؟**

شما می‌توانید تنها با استفاده از چند پست الکترونیک ساده، عملیات مرورگر وب و برخی

ضد ویروس‌ها، از رایانه خود محافظت کنید. شکی نیست که اینترنت می‌تواند مکان جالب و سرگرم‌کننده‌ای برای کشف کردن باشد، اما در نظر داشته باشید که ویروس‌های رایانه‌ای نیز آنجا سیر می‌کنند و قادر خواهند بود صدمه‌های جبران‌ناپذیری را به رایانه شما وارد سازند.

اگر ویروسی به دستگاه شما وارد شود، ممکن است نرم‌افزاری را پاک کرده و یا به آن آسیب جدی برساند. حتی ویروس تازه وارد، می‌تواند به رایانه دوستان و همکاران شما نیز، منتقل شود.

ویروس چیست؟

ویروس‌های رایانه‌ای، بسیار شبیه به ویروسی که در دانش پزشکی از آن صحبت می‌شود، هستند و می‌توانند در اندازه و شکل‌های مختلف باشند. قابل توجه است که بدانید یک ویروس رایانه‌ای، ممکن است، نشانه‌های متفاوتی را در دستگاه شما از خود بر جای گذارد. به‌طور کلی ویروس، برنامهٔ کوچکی است که در خود توانایی کپی شدن، از جایی به جای دیگر را دارد. ویروس‌ها به‌طور معمول، همراه پست الکترونیک و یا پنهان شدن در کد برخی از برنامه‌ها، وارد رایانه شما می‌شوند. بد نیست که بدانید، ویروس‌ها بری انتقال به رایانهٔ دوستان شما، از خود کپی کرده و نیز برخی از آنها، فایل‌های دستگاه را از بین می‌برند و یا دست‌کم در نرم‌افزار شما اختلال ایجاد می‌کنند.

چگونگی باخبرشدن از وجود ویروس

آگاه باشید که هر اختلال و بی‌نظمی در رایانه شما، نشان از وجود ویروس نیست، اما باید بدانید ویروس‌ها، همواره خود را از دید شما پنهان می‌سازند.

اگر دست‌کم یک و یا چند نشانه را که در این قسمت بیان شده است، در رایانهٔ خود مشاهده کردید، یقین داشته باشید که دستگاه شما ویروسی شده است.

۱. کم شدن بیش از حد معمول سرعت رایانه؛

۲. از کار افتادن دیسکی که همیشه در دستگاه به درستی کار می‌کرده است؛
۳. آهسته باز شدن برنامه و یا از بین رفتن برنامه‌ها در هنگام باز شدن؛
۴. تغییر اندازه، نام و اطلاعات فولدرها؛
۵. کاهش چشمگیر سرعت نصب برنامه؛
۶. اتفاقات عجیب در صفحهٔ نمایش.

انتشار ویروس

از آنجایی‌که برخی از ویروس‌ها، به‌وسیلهٔ پست الکترونیک منتقل می‌شوند، پیش از گشودن پیام‌های جدید، مطمئن شوید که ارسال‌کنندهٔ پیام را می‌شناسید و فایل پیوندزده شده به نامه را امتحان کنید.

درست است که ویروس‌ها همراه پست الکترونیک، از رایانه‌ای به رایانهٔ دیگر منتقل می‌گردند، اما آنها تنها می‌توانند با پیام‌هایی که فایل پیوندزده شده دارند، جابه‌جا شوند. دقت کنید فایل‌های دارای پیوست، ناقلان ویروس هستند.

فایل دارای پیوست، معمولاً به شکل گیرهٔ کاغذ و یا تصویر کوچکی از قطعه‌ای کاغذ یا پرونده، نشان داده می‌شود. این فایل می‌تواند یک تصویر، متن نگاشته‌شده و یا یک گیرهٔ متحرک باشد.

اگر آدرس E-mail فرد فرستندهٔ پیام برای شما ناآشنا باشد، باید دربارهٔ محتویات آن فایل احتیاط کنید. چنانچه پیام، مهم به‌نظر نمی‌رسید، از باز کردن آن صرفنظر کنید.

ویروس در فهرست آدرس‌های رایانه‌ای

افرادی که برای دیگران ویروس ارسال می‌کنند، قصد دارند با استفاده از شگردهای گوناگون، دریافت‌کنندهٔ پیام را به باز کردن فایل پیوست‌شده، ترغیب کنند.

دقت کنید که پیام با داشتن نامی تحریک‌کننده چون: «مهم»، «بدون اتلاف وقت بخوانید»،

ظاهری شبیه به لطیفه و یا تصویرهای جذاب، ما را به باز کردن فایل پیوندزده شده، وا می‌دارد.

اگر نشانی دوست و همکار خود را در پیام تشخیص دادید، اما متوجه نشدید که فایل پیوست‌شده چیست، پیش از باز کردن فایل با دوست خود تماس تلفنی بگیرید و تنها پس از اطمینان یافتن از سلامت محتویات پیام، آنرا بگشایید.

انتشار برخی از ویروس‌ها با سرعت بیشتری انجام می‌شود. آنها به تمام آدرس‌های موجود در فهرست آدرس‌های پست الکترونیک رایانه، فرستاده شده و بدون اتلاف زمان، دستگاه دوستان و همکاران شما را آلوده می‌سازند.

متأسفانه این امکان وجود دارد که پیام حامل ویروس از سوی دوست خود را بدون اینکه او کوچک‌ترین مطلبی در این‌باره بداند، دریافت کنید. تنها کافی است که آن فایل را باز کنید تا رایانه خود، دوستان و همکاران شما آلوده گردد.

اکنون، پس از مطالعهٔ مطالب بالا، دریافتید که چگونه ویروس‌ها از راه اینترنت منتشر شده و آسیب‌های جبران‌ناپذیری را به ارمغان می‌آورند. شما می‌توانید با بررسی برخی از نرم‌افزارهای ویزهٔ ضدویروس، مناسب‌ترین راه رهایی یافتن از این بلای اینترنتی را پیدا کنید.

وظیفهٔ نرم‌افزارهای ضدویروس، درست مانند سیستم ایمنی بدن، دفاع در برابر آسیب‌های ناشی از ویروس‌ها است. کار این نرم‌افزار، نظارت بر فعالیت‌های شما در اینترنت بوده و همواره در حال پیدا کردن ویروس‌های اینترنتی است. چنانچه ویروسی در فایل پیوندزده به پست الکترونیکی، پنهان شده و یا در اینترنت باشد، نرم‌افزار مربوطه مانع فعال شدن آن گردیده و از آسیب دیدن رایانه جلوگیری می‌کند. بیشتر ضدویروس‌ها به خودی خود، پیام‌های الکترونیکی دریافت‌شدهٔ شما را کنترل می‌کنند.

شما می‌توانید نرم‌افزار ضدویروس را از اینترنت Download کرده و یا از فروشگاه‌های ویژهٔ کامپیوتر، تهیه کنید.

ـ مفاهیم خود را به‌روز کنید. از آنجایی‌که همواره ویروس‌های جدیدتری آفریده می‌شوند،

تکنولوژی ضدویروس‌ها همیشه بدون اشکال نیستند. در این صورت آگاه باشید که نرم‌افزار ضدویروس خود را به‌روز کنید تا خطری رایانهٔ شما را تهدید نکند.

ـ هر ویروس، مفهوم ویژه‌ای دارد و شرکت‌های تولیدکنندهٔ نرم‌افزار ضدویروس، مفاهیم تازه‌ای برای مبارزه با ویروس می‌آفرینند که تنها برای محافظت از رایانهٔ شما است.

ـ دقت داشته باشید که همواره از مفاهیم به‌روز استفاده کرده تا از خطر آلوده شدن توسط ویروس‌های جدید مصون بمانید.

ـ اگر قصد کار کردن به دور از نگرانی آلوده شدن کامپیوتر خود را دارید، دست‌کم هر ماه مفاهیم خود را به‌روز کنید.

ـ از مایکروسافت به‌روز استفاده کنید. شرکت مایکروسافت، نرم‌افزارهای به‌روزی را در اختیار کاربران خود قرار داده است.

معمولاً ویروس‌ها برای منتشر شدن در جست‌وجوی نقصی در امنیت مرورگر و پست الکترونیک هستند. هنگامی‌که شرکت‌های بزرگ کامپیوتری چون مایکروسافت، از وجود چنین کاستی‌هایی باخبر می‌شوند، راه‌های برطرف کردن آنها را در اختیار کاربران خود قرار می‌دهند.

عوامل خطرناک

ممکن است پس از خواندن مطالب بالا از کار کردن با اینترنت، احساس خطر و نگرانی کنید، اما به‌خاطر داشته باشید که تمام ویروس‌ها خطرناک نیستند. بسیاری از آنها به دور از بر جای گذاشتن کوچک‌ترین نشان، پیوسته در حال انتقال یافتن از رایانه‌ای به رایانهٔ دیگر هستند. شما باید از ویروس‌هایی بهراسید که توسط آنها تمامی برنامه‌های خود را از دست می‌دهید. با نصب کردن یک نرم‌افزار ضدویروس مطمئن، لذت کار کردن با اینترنت را برای خود حفظ کرده و تمامی یادداشت‌های نوشته‌شده دربارهٔ ویروس‌ها را باور نکنید. متأسفانه بسیاری از داستان‌هایی که دربارهٔ ویروس‌ها به گوش شما می‌رسد، هیچ نشانی از واقعیت ندارند.

خود را حفظ کنید

حتی اگر مفاهیم خود را به‌روز کرده و از ضدویروس‌ها استفاده می‌کنید، باید شما نیز در محفوظ نگاه‌داشتن برنامه‌های باارزش خود کوشا باشید. بهترین راه برای حفظ کردن اسناد و نوشته‌های مهم، تهیهٔ فایل‌های پشتیبان از آنهاست.

در صورت داشتن فایل‌های پشتیبان، چنانچه ویروسی رایانهٔ شما را آلوده کند و اطلاعات خود را از دست بدهید، پس از برطرف کردن ویروس قادر خواهید بود تمام برنامه‌ها را بازآفرینی کنید.

راه‌های طلایی

در این قسمت بهترین راه‌های محافظت کردن از رایانه در برابر ویروس‌ها بیان شده است؛

۱. یک برنامهٔ ضدویروس در رایانهٔ خود نصب کنید.

۲. هیچ‌گاه فایل پیوندزده شده به پست الکترونیک را ناخودآگاه نگشایید.

۳. برنامه و نرم‌افزار موردنیاز خود را از منابع قابل اعتماد و معتبر تهیه کنید.

۴. از جدیدترین سیستم عامل استفاده کنید.

۵. از فایل‌های باارزش خود،فایل‌های پشتیبان تهیه کنید.

۶. به‌روز باشید.

ـ استراتژی حفاظت از اطلاعات شبکه‌های کامپیوتری

اطلاعات در سازمان‌ها و مؤسسات مدرن به منزلهٔ شاهرگ حیاتی محسوب می‌شوند. دستیابی به اطلاعات و عرضه مناسب و سریع آن، همواره مورد توجه سازمان‌هایی است که اطلاعات در آنها دارای نقشی محوری و سرنوشت‌ساز است. سازمان‌ها و مؤسسات باید یک زیرساخت مناسب اطلاعاتی را برای خود ایجاد و در جهت انضباط اطلاعاتی در سازمان خود حرکت نمایند.

اگر می‌خواهیم ارائه‌دهنده اطلاعات در عصر اطلاعات بوده و صرفاً مصرف‌کننده اطلاعات نباشیم، در مرحله نخست باید فرآیندهای تولید، عرضه و استفاده از اطلاعات را در سازمان خود قانونمند نموده و در مراحل بعد، امکان استفاده از اطلاعات ذی‌ربط را برای متقاضیان (محلی و جهانی) در سریع‌ترین زمان ممکن فراهم نماییم. سرعت در تولید و عرضه اطلاعات ارزشمند، یکی از رموز موفقیت سازمان‌ها و مؤسسات در عصر اطلاعات است. پس از ایجاد انضباط اطلاعاتی، باید با بهره‌گیری از شبکه‌های کامپیوتری زمینه استفاده قانونمند و هدفمند از اطلاعات را برای سایرین فراهم کنیم. اطلاعات ارائه‌شده می‌تواند به‌صورت محلی (اینترانت) و یا جهانی (اینترنت) مورد استفاده قرار گیرد. فراموش نکنیم در این هنگامه اطلاعاتی، مصرف‌کنندگان اطلاعات دارای حق مسلم انتخاب هستند و در صورتی‌که سازمان و یا مؤسسه‌ای در ارائه اطلاعات سهواً و یا تعمداً دچار اختلال و یا مشکل شود، دلیلی بر توقف عملکرد مصرف‌کنندگان اطلاعات تا برطرف نمودن مشکل ما، وجود نخواهد داشت. سازمان‌ها و مؤسسات باید خود را برای نبردی سخت در عرضه و ارائه اطلاعات آماده کنند و در این راستا علاوه بر پتانسیل‌های سخت‌افزاری و نرم‌افزاری استفاده‌شده، از تدبیر و دوراندیشی نیز فاصله نگیرند. در میدان عرضه و ارائه اطلاعات، کسب موفقیت نه به‌دلیل ضعف دیگران بلکه بر توانمندی ما استوار خواهد بود. مصرف‌کنندگان اطلاعات، به‌طور قطع ارائه‌دهندگان اطلاعاتی را برمی‌گزینند که نسبت به توان و پتانسیل آنان اطمینان حاصل کرده باشند. آیا سازمان ما در عصر اطلاعات به پتانسیل‌های لازم در این خصوص دست یافته است؟ آیا در سازمان ما بستر و ساختار مناسب اطلاعاتی ایجاد شده است؟ آیا گردش امور در سازمان ما مبتنی بر یک سیستم اطلاعاتی مدرن است؟ آیا سازمان ما قادر به تعامل اطلاعاتی با سایر سازمان‌ها است؟ آیا در سازمان ما نقاط تماس اطلاعاتی با دنیای خارج از سازمان تدوین شده است؟ آیا فاصله تولید و استفاده از اطلاعات در سازمان ما به حداقل مقدار خود رسیده است؟ آیا اطلاعات قابل عرضه سازمان ما، در سریع‌ترین زمان و با کیفیتی مناسب در اختیار مصرف‌کنندگان متقاضی قرار می‌گیرد؟ حضور یک سازمان در عرصه جهانی، صرفاً داشتن یک

وب سایت با اطلاعات ایستا نخواهد بود. امروزه میلیون‌ها وب سایت بر روی اینترنت وجود دارند که هر روز نیز بر تعداد آنان افزوده می‌شود.

کاربران اینترنت برای پذیرش سایت سازمان ما، دلایل موجهی را دنبال خواهند کرد. در این هنگامه داشتن سایت و راه‌اندازی سایت، اصل موضوع که همانا ایجاد یک سازمان مدرن اطلاعاتی است، فراموش نشود. سازمان ما در این راستا چگونه حرکت کرده و مختصات آن در نقشه اطلاعاتی یک سازمان مدرن چیست؟ بدیهی است، ارائه‌دهندگان اطلاعات خود در سطوحی دیگر به مصرف‌کنندگان اطلاعات تبدیل و مصرف‌کنندگان اطلاعات، در حالات دیگر خود می‌توانند به‌عنوان ارائه دهنده اطلاعات مطرح شوند. مصرف بهینه و هدفمند اطلاعات در صورتی‌که به افزایش آگاهی، تولید و ارائه اطلاعات ختم شود، امری بسیار پسندیده خواهد بود. در غیر این صورت، مصرف مطلق و همیشگی اطلاعات بدون جهت‌گیری خاص، بدترین نوع استفاده از اطلاعات بوده که به‌طور قطع به سرانجام مطلوبی ختم نخواهد شد.

شبکه‌های کامپیوتری

در صورتی‌که قصد ارائه و یا حتی مصرف بهینه و سریع اطلاعات را داشته باشیم، باید زیرساخت مناسب را در این جهت ایجاد کنیم. شبکه‌های کامپیوتری، بستری مناسب برای عرضه، ارائه و مصرف اطلاعات به‌شمار می‌روند (دقیقاً مشابه نقش جاده‌ها در یک سیستم حمل‌ونقل). عرضه، ارائه و مصرف یک کالا نیازمند وجود یک سیستم حمل‌ونقل مطلوب خواهد بود. در صورتی‌که سازمان و یا مؤسسه‌ای محصولی را تولید کرده، اما قادر به عرضه آن در زمان مناسب (قبل از اتمام تاریخ مصرف) برای متقاضیان نباشد، به‌طور قطع از سازمان‌هایی که تولیدات خود را با بهره‌گیری از یک زیرساخت مناسب، به سرعت در اختیار متقاضیان قرار می‌دهند، عقب خواهند افتاد. شاید به همین دلیل باشد که وجود جاده‌ها و زیرساخت‌های مناسب ارتباطی، به‌عنوان یکی از دلایل موفقیت برخی از کشورها در عصر انقلاب صنعتی، ذکر می‌شود. فراموش نکنیم که امروزه زمان کهنه شدن اطلاعات از زمان تولید اطلاعات بسیار

سریع‌تر بوده و باید قبل از اتمام تاریخ مصرف اطلاعات با استفاده از زیرساخت مناسب (شبکه‌های ارتباطی) اقدام به عرضه آنان نمود. برای عرضه اطلاعات می‌توان از امکاناتی دیگر نیز استفاده کرد، اما قطعاً شبکه‌های کامپیوتری به‌دلیل سرعت ارتباطی بسیار بالا دارای نقشی کلیدی و منحصر به فرد هستند، مثلاً می‌توان مشخصات کالا و یا محصول تولیدشده در یک سازمان را از طریق یک نامه به متقاضیان اعلام کرد، اما در صورتی‌که سازمانی در این راستا از گزینه پست الکترونیکی استفاده نماید، به‌طور قطع متقاضیان مربوطه در زمانی بسیار سریع‌تر نسبت به مشخصات کالای تولیدشده، آگاهی پیدا خواهند کرد.

امنیت اطلاعات در شبکه‌های کامپیوتری

به موازات حرکت به سمت یک سازمان مدرن و مبتنی بر تکنولوژی اطلاعات، باید تدابیر لازم در رابطه با حفاظت از اطلاعات نیز اندیشیده شود. مهم‌ترین مزیت و رسالت شبکه‌های کامپیوتری، اشتراک منابع سخت‌افزاری و نرم‌افزاری است. کنترل دستیابی و نحوه استفاده از منابع به اشتراک گذاشته‌شده از مهم‌ترین اهداف یک سیستم امنیتی در شبکه است. با گسترش شبکه‌های کامپیوتری خصوصاً اینترنت، نگرش نسبت به امنیت اطلاعات و سایر منابع به اشتراک گذاشته‌شده، وارد مرحله جدیدی گشته است. در این راستا، ضروری است که هر سازمان برای حفاظت از اطلاعات ارزشمند، پایبند به یک استراتژی خاص بوده و براساس آن سیستم امنیتی را اجرا و پیاده‌سازی نماید. عدم ایجاد سیستم مناسب امنیتی می‌تواند پیامدهای منفی و دور از انتظاری را به‌دنبال داشته باشد. استراتژی سازمان ما برای حفاظت و دفاع از اطلاعات چیست؟ در صورت بروز مشکل امنیتی در رابطه با اطلاعات در سازمان، به‌دنبال کدامین مقصر می‌گردیم؟ شاید اگر در چنین مواردی، تمام مسائل امنیتی و مشکلات به‌وجود آمده را به خود کامپیوتر نسبت دهیم، بهترین امکان برون رفت از مشکل به‌وجود خواهد آمد، چراکه کامپیوتر توان دفاع کردن از خود را ندارد. آیا واقعاً روش و نحوه برخورد با مشکل به‌وجود آمده چنین است؟ در حالیکه یک سازمان برای خرید سخت‌افزار نگرانی‌های خاص

خود را داشته و سعی در برطرف نمودن معقول آنها دارد، آیا برای امنیت و حفاظت از اطلاعات نباید نگرانی به مراتب بیشتری در سازمان وجود داشته باشد؟

استراتژی

دفاع در عمق، عنوان یک استراتژی عملی به‌منظور نیل به تضمین و ایمن‌سازی اطلاعات در محیط‌های شبکه امروزی است. استراتژی فوق، یکی از مناسب‌ترین و عملی‌ترین گزینه‌های موجود است که متأثر از برنامه‌های هوشمند برخاسته از تکنیک‌ها و تکنولوژی‌های متفاوت، تدوین می‌گردد. استراتژی پیشنهادی، بر سه مؤلفه متفاوت ظرفیت‌های حفاظتی، هزینه‌ها و رویکردهای عملیاتی تأکید داشته و توازنی معقول بین آنها را برقرار می‌نماید. در این مقاله به بررسی عناصر اصلی و نقش هر یک از آنان در استراتژی پیشنهادی، پرداخته خواهد شد.

دشمنان، انگیزه‌ها و انواع حملات اطلاعاتی

به‌منظور دفاع مؤثر و مطلوب در مقابل حملات به اطلاعات و سیستم‌های اطلاعاتی، یک سازمان باید دشمنان، پتانسیل و انگیزه‌های آنان و انواع حملات را به درستی برای خود آنالیزکرده تا از این طریق دیدگاهی منطقی نسبت به موازین فوق ایجاد و در ادامه امکان برخورد مناسب با آنان فراهم شود. اگر قصد تجویز دارو برای بیماری وجود داشته باشد، به‌طور قطع قبل از معاینه و آنالیز وضعیت بیمار، اقدام به تجویز دارو برای وی نخواهد شد. در چنین مواردی نمی‌توان برای برخورد با مسائل پویا از راه‌حل‌های مشابه و ایستا استفاده کرد. به‌منظور ارائه راهکارهای پویا و متناسب با مسائل متغیر، ضروری است در ابتدا نسبت به کالبدشکافی دشمنان، انگیزه‌ها و انواع حملات، شناخت مناسبی ایجاد شود.

دشمنان شامل: سارقان اطلاعاتی، مجرمان، دزدان کامپیوتری، شرکت‌های رقیب و غیره هستند.

انگیزه‌های موجود نیز شامل: جمع‌آوری هوشمندانه، دستبرد فکری (عقلانی)، عدم پذیرش

سرویس‌ها، کنف کردن، احساس غرور و مورد توجه واقع شدن هستند.

انواع حملات شامل: مشاهده غیرفعال ارتباطات، حملات به شبکه‌های فعال، حملات از نزدیک (مجاورت سیستم‌ها)، سوءاستفاده و بهره‌برداری خودی‌ها (محرمان) و حملات مربوط به ارائه‌دهندگان صنعتی یکی از منابع تکنولوژی اطلاعات است.

سیستم‌های اطلاعاتی و شبکه‌های کامپیوتری اهداف مناسب و جذابی برای مهاجمان اطلاعاتی هستند. بنابراین لازم است، تدابیر لازم در خصوص حفاظت سیستم‌ها و شبکه‌ها در مقابل انواع متفاوت حملات اطلاعاتی اندیشیده شود. به‌منظور آنالیز حملات اطلاعاتی و اتخاذ راهکار مناسب به‌منظور برخورد با آنان، لازم است در ابتدا با انواع حملات اطلاعات آشنا شده تا از این طریق امکان برخورد مناسب و سیستماتیک با هر یک از آنان فراهم گردد. به‌طور قطع، وقتی ما شناخت مناسبی را نسبت به نوع و علل حمله داشته باشیم، قادر به برخورد منطقی با آن به‌گونه‌ای خواهیم بود که پس از برخورد، زمینه تکرار موارد مشابه حذف شود. انواع حملات اطلاعاتی به‌شرح ذیل است؛

- غیرفعال
- فعال
- نزدیک (مجاور)
- خودی‌ها (محرمان)
- عرضه (توزیع)

ویژگی هر یک از انواع حملات فوق، به‌شرح ذیل است:

غیرفعال[1]: این نوع حملات شامل؛ آنالیز ترافیک شبکه، شنود ارتباطات حفاظت‌نشده، رمزگشایی ترافیک‌های رمزشده ضعیف و به‌دست آوردن اطلاعات معتبری همچون رمز عبور است. رهگیری غیرفعال عملیات شبکه، می‌تواند به مهاجمان، هشدارها و اطلاعات لازم را در خصوص عملیات قریب‌الوقوعی که قرار

1. Passive

است در شبکه اتفاق بیفتد (قرار است از مسیر فوق در آینده محموله‌ای ارزشمند عبور داده شود) را بدهد. پیامدهای این نوع حملات، آشکار شدن اطلاعات و یا فایل‌های اطلاعاتی برای یک مهاجم، بدون رضایت و آگاهی کاربر خواهد بود.

فعال[1]: این نوع حملات شامل؛ تلاش در جهت خنثی نمودن و یا حذف ویژگی‌های امنیتی، معرفی کدهای مخرب، سرقت و یا تغییر دادن اطلاعات می‌شود. حملات فوق، می‌توانند از طریق ستون فقرات یک شبکه، سوءاستفاده موقت اطلاعاتی، نفوذ الکترونیکی در یک قلمرو بسته و حفاظت‌شده و یا حمله به یک کاربر تأییدشده در زمان اتصال به یک ناحیه بسته و حفاظت‌شده، بروز کند. پیامد حملات فوق، افشای اطلاعات، اشاعه فایل‌های اطلاعاتی، عدم پذیرش سرویس و یا تغییر در داده‌ها خواهد بود.

مجاور[2]: این نوع حملات توسط افرادی که در مجاورت (نزدیکی) سیستم‌ها قرار دارند با استفاده از تسهیلات موجود و با ترفندی خاص به‌منظور نیل به اهدافی نظیر؛ اصلاح، جمع‌آوری و انکار دستیابی به اطلاعات باشد، صورت می‌پذیرد. حملات مبتنی بر مجاورت فیزیکی از طریق ورود مخفیانه، دستیابی باز و یا هر دو انجام می‌شود.

خودی[3]: حملات خودی‌ها، می‌تواند به‌صورت مخرب یا غیرمخرب جلوه کند. حملات مخرب از این نوع شامل؛ استراق‌سمع تعمدی، سرقت و یا آسیب‌رسانی به اطلاعات، استفاده از اطلاعات به طرزی کاملاً شیادانه و فریب‌آمیز و یا رد دستیابی سایر کاربران تأییدشده باشد. حملات غیرمخرب از این نوع، عموماً به‌دلیل سهل‌انگاری (حواس‌پرتی)، فقدان دانش لازم و یا سرپیچی عمدی از سیاست‌های امنیتی صورت می‌پذیرد.

توزیع[4]: حملات از این نوع شامل، کدهای مخربی است که در زمان تغییر سخت‌افزار و یا نرم‌افزار در محل مربوطه (کارخانه و شرکت) و یا در زمان توزیع آنها (سخت‌افزار و نرم‌افزار) جلوه می‌کند. این نوع حملات می‌توانند، کدهای مخربی

1. Active
2. Close-in
3. Insider
4. Distribution

را در بطن یک محصول جاسازی نمایند، نظیر یک درب از عقب[1] که امکان دستیابی غیرمجاز به اطلاعات و یا عملیات سیستم در زمان آتی را به‌منظور سوءاستفاده اطلاعاتی فراهم می‌نماید. در این رابطه لازم است به سایر موارد نظیر آتش‌سوزی، سیل، قطع برق و خطای کاربران نیز توجه خاصی مبذول شود.

1. Back Door